Nuclear Verification's Holy Grail:

Verifying Nuclear Warheads — a new approach

CNS
OCCASIONAL PAPER
#64 · DECEMBER 2024

Miles Pomper, William Moon, Marshall Brown, Ferenc Dalnoki Veress, Dan Zhukov, Dick Gullickson, and Yanliang Pan

With a Foreword by the Hon. Rose Gottemoeller

Middlebury Institute *of* International Studies at Monterey
James Martin Center for Nonproliferation Studies

Nuclear Verification's Holy Grail:

Verifying Nuclear Warheads — a new approach

Miles Pomper, William Moon, Marshall Brown, Ferenc Dalnoki-Veress, Dan Zhukov, Dick Gullickson, and Yanliang Pan

With a Foreword by the Hon. Rose Gottemoeller

James Martin Center of Nonproliferation Studies
Middlebury Institute of International Studies at Monterey

460 Pierce Street, Monterey, CA 93940, USA
Phone: +1 (831) 647-4154
Fax: +1 (831) 647-3519

www.nonproliferation.org **www.middlebury.edu/institute**

This work was performed under contract (19AQMM22P1065) with the U.S. Department of State.

The views, judgments, and conclusions in this report are the sole representations of the authors and do not necessarily represent either the official position or policy or bear the endorsement CNS or the Middlebury Institute of International Studies at Monterey.

Contents

Contents continued...

Contents continued...

Foreword

Rose Gottemoeller

This study is the culmination of four years of work to think through what would be required to track and monitor nuclear warheads in a verification process. It first began in 2021, shortly after President Joe Biden of the United States and President Vladimir Putin of Russia extended the New START Treaty until February 2026; the two presidents also announced the launch of bilateral strategic stability talks. This positive moment in the U.S.-Russian relationship, which became almost unimaginable after the 2022 Russian invasion of Ukraine, was the original impetus for the project. It also launched in the aftermath of the U.S. withdrawal from the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles, commonly known as the INF Treaty. The Russians had been violating the Treaty with the production and deployment of the 9M729 missile, also known in NATO parlance as the SSC-8. All NATO allies concurred with the withdrawal, which the United States completed in August 2019.

The effort began with two strands of activity. The study team knew that when the United States and Russia decided to return to the negotiating table, the United States would place a high priority on seeking direct limits on warheads. Prior treaties had focused on controlling and eliminating missiles but had not focused directly on the warheads that armed them. It had long been a goal of the United States to seek direct limits on warheads, in order to more accurately constrain a Russian preponderance in warheads designated for theater- and shorter-range systems.[1] However, if such an agreement were negotiated, the European allies would be ill-equipped to participate. On-site inspections under the INF Treaty had ended on May 31, 2001, so it had been twenty years since the allies had had to participate in verification activities. Most had lost expertise and institutional memory; some had never participated at all. “Raising the IQ” of the NATO allies about participating in arms control implementation was thus the first strand of activity.

The second strand grew up around a conviction in the study team that the well-practiced verification techniques that had been exercised in INF and strategic arms control treaties since the 1980s could be augmented with new technology and innovative techniques. Thus emerged the emphasis on using cryptography to underpin a unique warhead tracking system. This work took advantage of some of the finest experts in the field of cryptography at Stanford University, and also the extensive experience gained during the Defense Threat Reduction Agency’s many years of work to strengthen warhead protection, control and accounting in Russian Ministry of Defense nuclear warhead storage facilities. This work, which spanned a period of over fifteen years from 1995-2013, provided the study team with a great depth of knowledge about the normal operating procedures in Russian military warhead facilities. This deep knowledge was

[1] The Resolution of Ratification of the New START Treaty placed this requirement into U.S. law. https://www.congress.gov/treaty-document/111th-congress/5/resolution-text

vital to developing a concept for the tracking system, providing it with a realism and accuracy that otherwise would not have been possible.

These two strands of work culminated in 2022 in a significant study, “Everything Counts: Building a Control Regime for Non-Strategic Nuclear Warheads in Europe.”[2] However, the team realized that only one element of warhead verification had been touched—the broad outlines of a system for maintaining and exchanging information over the life of an agreement. Other verification elements such as on-site inspections and particular verification technologies had not been considered. They therefore resolved to expand the scope of work to imagine an entire closed system for nuclear warhead verification. With the cryptographic element as its foundation, the team reviewed the extensive experience of treaties, agreements and other activities such as exhibitions and joint experiments that had been built up over the many years of U.S.-Soviet and Russian cooperation on nuclear weapons control. From this, they created a comprehensive menu of measures that could be considered for a future warhead control regime, calibrating the measures according to the level of their intrusiveness.

Intrusiveness is a key concept for any military establishment participating in an arms control regime to understand and accept. While the United States may seek maximum intrusiveness to be assured that the Russians or other counterparts are not cheating on an agreement, the U.S. Air Force and Navy will want to calibrate that intrusiveness to sustain their operational flexibility and timeliness.

Arms control regimes must be completely reciprocal for all parties to agree to them. Therefore, whatever intrusive techniques are applied to Russian facilities will also have to be endured in U.S. Air Force and Navy facilities. If the measures slow or interrupt operational tempo too much, then they become unacceptable. Likewise—especially where warheads are concerned—if the measures provide too much sensitive information about U.S. warhead capabilities, then they also become unacceptable, to their Department of Energy and Department of Defense stewards but also to the entire U.S. government.

Thus, negotiators must seek a balance of intrusiveness and tolerance for operational and secrecy requirements. This balance will be a vital goal for any future agreement that attempts to directly limit warheads.

Although the prospects for nuclear controls and limitations have retreated into the distance with the advent of Russia’s war against Ukraine, Cold War history teaches that the appetite for negotiation can change at any time. Because the war in Ukraine has produced a massive proliferation in the deployment and operational use of intermediate- and shorter-range missiles, an urge to negotiate constraints on them might emerge fairly soon, out of near-term negotiations to end the war. From the U.S. perspective, warheads controls will be a necessary component.

The easiest constraint to describe in agreement text if not to implement would be a total ban on nuclear-armed missiles of all ground-based types used in this war, whether Russian, Ukrainian or NATO in origin. No one has an interest in the wide number of drones, cruise and ballistic missiles launched daily in this war being nuclear-armed. A total ban on nuclear-armed intermediate- and

[2] https://nonproliferation.org/op55-everything-counts-building-a-control-regime-for-nonstrategic-nuclear-warheads-in-europe/

shorter-range ground-based missiles might therefore be a goal of the peace talks between Russia and Ukraine, with NATO also participating. In that case, this study is an excellent compendium, or menu, of warhead monitoring measures that could be considered to implement the ban.

One great advantage of this study has been the interdisciplinary and intergenerational nature of the team that carried it out. The lead substantive players were the most experienced manager of the DTRA warhead programs in Russia, William Moon and a top U.S. arms control treaty lawyer, Marshall Brown. Understanding of the Soviet/Russian point of view was provided by Nikolai Sokov, a leading expert with many years of arms control negotiating experience in the Soviet and Russian Ministries of Foreign Affairs. Technical expertise on warhead monitoring was provided by Ferenc Dalnoki-Veress, a master of technical possibility. And the younger generation of cryptographic and nuclear experts was ably represented by Neil Perry, Daniil Zhukov, and Yanliang Pan, who contributed significantly to the technical success of the project. All of this action was ably orchestrated by Miles Pomper, who led the project from its outset and provided its strategic direction. For me, it has been a huge privilege to work with this team.

I. Overview

While verification in previous arms control agreements between the United States and Russia has focused largely on delivery systems, future agreements may seek to focus on the verification of limits on the warheads themselves, requiring innovative verification tools and protocols. In May 2022, CNS published Occasional Paper #55 *Everything Counts: Building a Control Regime for Nonstrategic Nuclear Warheads in Europe,* which put forward, inter alia, the concept of a warhead tracking system (WTS) using cryptographic identifiers and warhead logistics data from existing inventory management systems. A demonstration of the associated warhead verification approach took place in December 2022. Since then, CNS has advanced the WTS concept with the expectation that a data exchange methodology, including a system for data challenges and warhead notifications using cryptographically generated warhead unique identifiers, can provide a foundation from which to build a comprehensive verification protocol addressing nuclear warheads.

This paper presents a menu of verification methods, technologies, and measures that may be used to design a verification protocol for any type of warhead stockpile agreement ranging from: promoting transparency of overall stockpile levels; to introducing initial confidence building measures through the exchange of warhead stockpile data; to enabling notifications of warhead movements as a risk reduction measure; or to a formal arms control treaty that might cap or require reductions in the warhead inventory. The goal is to provide a variety of technologies and verification measures to maximize confidence in any agreed warhead data exchanges while minimizing on-site inspection requirements. The menu identifies specific verification measures and technologies that work together to provide the highest possible confidence level in the data and declarations issued by the inspected party. These measures and technologies have also been carefully selected to minimize the level of intrusiveness they may require.

All the measures identified in the menu have been carefully designed to minimize safety and security concerns as well as potential vulnerabilities from exposing warhead data involving design, composition, or performance. The menu includes on-site measures that range from a level of mild intrusiveness to highly intrusive techniques that could be used if the sides were to insist and agree upon on-site observation and exchange of warhead-related data obtained through on-site measures. While the on-site measures identified in our menus for the most part focus on collecting data from equipment used to handle or secure warheads, we also offer some optional measures that could be used to verify the presence or absence of warheads in certain containers, transportation systems, or storage locations, though these measures would all be considered highly intrusive on our spectrum of intrusiveness.

In defining "intrusiveness" within our assessment, we considered a variety of factors including, but not limited to: a.) physical presence of inspectors with the degree of intrusiveness increasing from being in the country, to traveling to a base, or to the most intrusive, permitting inspectors direct access to a warhead; b.) sensitivity and vulnerability of the collected data; c.) cost to the host country; and, d.) the complexity of the technology. The degree of intrusiveness also depends on several factors in designing and implementing the overall systems to be used in monitoring warhead transport and handling systems: how much data are collected; whether the data are collected in real time or collected at designated intervals of time; and how the data are collected – on site by the inspection team, by representatives of the host country as observed by the inspection team in real time, or by the host country at designated intervals. Intrusiveness would also depend on where the data are collected – for example, at a designated neutral site, at a declared parking area, or at specific locations along a route. Finally, intrusiveness could be mitigated if the data are collected and conveyed via a hash code or shared openly. **Annex A** provides an assessment of the intrusiveness of the measures and technologies in our menu.

In addition, our menu **(Annex B)** identifies arms control precedents related to each verification measure. For this part of our analysis, we included formal arms control agreements, joint experiments and exercises, and US-Russian military-to-military and Cooperative Threat Reduction (CTR) engagements. These precedents also include a thorough review of current and former verification research and development (R&D) programs conducted by the Department of Energy (DOE)/National Nuclear Security Administration (NNSA), the national labs, Department of Defense (DoD)/Defense Threat Reduction Agency (DTRA), and the State Department, as well as international R&D programs, including those supported by the International Atomic Energy Agency (IAEA), the International Partnership for Nuclear Disarmament Verification (IPNDV), and previous joint R&D programs conducted between the US and Russia.

Annex C provides a draft verification protocol based on the verification methods, technologies, and measures described in this paper. This draft protocol should be seen as the representation, in legal form, of one possible approach to nuclear warhead verification, but with the understanding that this text would require modification based on the substance and legal status of the associated agreement addressing nuclear warheads, as well as any other agreements relating to the verification methods, technologies and measures that may be reached by the sides during technical discussions.

Annex D provides recommendations for joint technical discussions and activities related to the draft verification protocol, including preparatory steps, such as those that could be conducted prior to entry into force of an arms control agreement on nuclear warheads. Annex D also describes several enhanced verification measures that could be considered, in addition to those contained in the draft verification protocol, to validate a baseline data exchange and to monitor compliance over time.

No verification will be 100 percent effective against all potential cheating. The goal of a verification system is to create a high probability of detecting a significant violation. This has been the U.S. approach since the 1970s. An attempt to imagine every theoretically possible way to commit a small violation and detect it with high probability would be immensely difficult to negotiate and even more difficult to implement. The key finding in this study is that it is possible to design a combination of measures to provide high confidence in the validity of data exchanges on warhead stockpiles without requiring a high level of intrusiveness and with minimal on-site requirements. Recognizing that such an approach may lead to concerns that cheating will occur in the absence of greater intrusiveness, **Annex E** describes two scenarios that demonstrate how the other party may seek to violate the agreement and show how such attempts would be detected and thwarted using the measures included in the verification protocol, as enhanced by verification measures described in **Annex D**. A secondary finding is that by using the WTS methodology, relatively simple and inexpensive technologies could be used to achieve high verification confidence. These technologies would only require limited R&D to enhance their tamper protection and to determine how best to apply them to the requisite warhead handling and support equipment.

II: Warhead Tracking System ("WTS") and Warhead Passports

As nuclear warheads are relatively small and mobile, they cannot be identified and tracked using National Technical Means (NTM) such as military satellites. The technical and operational challenges posed by nuclear warheads require a data-exchange methodology that can track the lifetime of operations and transactions conducted for all warheads in the inventory. Warheads cannot be tracked by using a simple number or designator; they aren't easily distinguishable; and their changing composition and dynamic life cycle make them difficult to track.

The proposed WTS would leverage existing U.S and Russian inventory-management systems (DIAMONDS and AICMS) to support an agreement addressing nuclear warheads as a treaty-limited item. This methodology minimizes operational impacts while reducing errors and increasing confidence in the data that is processed from these systems. Much of the data used to track warheads consists of less sensitive historical, logistical data on warhead locations, movements, and transactions that have been exchanged between the U.S. and Russia under previous agreements and during CTR cooperation.

While much of the logistical data used by AICMS and DIAMONDS to track warheads has been exchanged, neither side would want to exchange all the data because sensitive information such as service life and reliability could be gleaned from a complete listing of all maintenance activity. Therefore, the WTS would use cryptography to represent the full set of data on individual warheads along with a data challenge process that would validate enough specific data points from a warhead's service life to build confidence in the overall inventory exchanges. WTS does this by using "warhead passports," which include all data and information required to monitor and track nuclear-warhead movements and operations. The data-exchange methodology would create a unique, virtual identifier for each warhead, derived from actual warhead data provided by the respective inventory-management systems. The identifier would be a cryptographic code representing the individual warhead's lifetime logistical data. Nuclear warhead passport combine data on location, transportation operations, components, escort personnel, and, potentially, warhead status into a virtual record that can serve to identify individual warheads.

Figure 1: Notional Warhead Passport

Date/Time	Location	Status	Components	Operation	Personnel	ID Hash
11-11-2001/4:00	Departure from Assembly-1	Inactive	Primary (P), Secondary (S), Limited Lifetime Component (LLC), Permissive Action Link (PAL)	Transfer of Custody (TOC): from Rosatom to MOD	Escort-1	8df91ks83v0
11-13-2001/6:15	Arrival RTP-1	Inactive	P, S, LLC, PAL	Rail to Road Transfer	Escort-1	
...	...	...	...	...	...	
1-02-2023/13:15	Central Storage Site-1	Active	P, S, LLC, PAL	Audit	Escort-4	
1-08-2023/2:06	Central Storage Site-1	Scheduled for dismantlement	P, S, LLC, PAL	Designated for dismantlement	Escort-11	b1s5oe25am
2-03-2023/12:40	RTP-5	Scheduled for dismantlement	P, S, PAL	Transportation	Escort-11	a832j3msy1s
2-05-2023/18:57	Disassembly-3	Dismantled	P, S, PAL	TOC, Disassembly	Escort-11	x98y1h3ni01

Note: The thick line divides the entries recorded before and after the commencement of the data exchange process. Baseline passport (above the line) is used in its entirety to derive and share a single commitment identifying the passport, while entries recorded during the process (below the line) are hashed and committed as individual status updates.

Like a fingerprint, each warhead will have a unique set of historical logistics and handling data associated with it that can be used to distinguish warheads so that they can be tracked under a warhead-verification agreement. When compiled together, warhead locations, transaction dates, components, personnel, and status provide a rich assortment of data elements within warhead-passport data that can be used to develop unique identifiers to monitor and track warheads over their life cycle in support of a verification methodology that uses cryptography to protect sensitive data sets while exchanging allowable data elements to validate warhead data.

Figure 2: WTS Data Challenge and Exchange Process

1. The host party derives a hash from a passport entry or a notification

2. The hash is committed to the observing party

3. Later, the observing party issues a data challenge for the commitment

4. The host party decommits the original passport entry or notification and shares it along with a cryptographic proof

5. The observing party validates the decommitted data by using the proof to derive a hash and comparing it to the original commitment

It is also important to note that the WTS would never report current logistical data that could be used to target warheads while being transported. Instead, it would use historical data, some of which may be validated by specific NTM or other data to validate elements within the warhead passports that can be exchanged.

III. Warhead Operations in a "Closed System"

Nuclear warheads exist within a closed system – they are strictly accounted for and can only be located only at certain facilities and transported subject to strict rules. The closed nature of that system creates an opportunity for accounting and verification. Warhead passports and the Warhead Tracking System (WTS), designed and demonstrated by CNS to a senior audience of arms control experts in December 2022,[3] leverage the closed nature of the nuclear enterprise and provide a foundation for this menu of verification measures.

There is a strong precedent for building accounting and verification around the principle of a closed system. Namely, START's Memorandum of Understanding only permits mobile ICBMs and their launchers to be located at or moved between designated facilities. With certain specified exceptions a mobile ICBM or its launcher outside such facilities would constitute a violation. Similarly, the missile enters accounting when it leaves the production facility and exits it when the missile is sent to the elimination or dismantlement facility. This proposed approach builds on the same principle but accounts for the more closed operational system for nuclear warheads and incorporates significantly stricter verification measures.

The menu of arms control verification measures presented in this paper integrates this closed system, warhead passports, and the WTS system to provide a comprehensive warhead verification approach that can support a potential future agreement or risk reduction measure addressing warhead stockpiles.

To fully understand the rationale behind the proposed approach, a brief review of the operational system of a nuclear warhead stockpile, including the equipment, personnel, logistics, and facilities is appropriate. Since the primary interest of the United States is accounting for the Russian stockpile, our study primarily focused on the Russian system for handling nuclear weapons. We sought, however, also to match the proposed regime to US practices to facilitate its implementation in a relevant international regime.

The key characteristic of the warhead operational system is that every element of the system is dedicated specifically to support nuclear warhead safety, security, and operations, and that all warhead transportation and handling equipment are secured within this system. We know this is true for the US and Russia based on military exchanges and nuclear security cooperation under the CTR program. To the best of our knowledge and research conducted thus far, we believe this is also true for China.

The warhead operational system consists of elements including, but not restricted to warheads and their components; containers; lifting and handling gear such as cranes and forklifts; transportation and moving systems such as gurneys, trucks, railcars, helicopters, and aircraft; temporary and permanent storage facilities; and related security

---

[3] Marshall L. Brown, Jr., "Demonstrating a Warhead Tracking System," James Martin Center for Nonproliferation Studies, March, 2023, https://nonproliferation.org/demonstrating-a-warhead-tracking-system/.

systems. For the purposes of this study, we focused on assembled warheads in the U.S. and Russian inventories. Warheads that are installed on operationally deployed strategic delivery systems are not directly addressed by the verification measures described in this study because verification procedures are already contained in the New START treaty, but the measures proposed by CNS are flexible and could be extended to these deployed warheads as well.

The first step in the warhead verification regime we propose begins with the transfer of custody of an assembled device from the respective production facility to the Russian Ministry of Defense or US Department of Defense, and that regime continues until the transfer of warheads to the operational nuclear forces in the Army, Navy, Air Force, or Strategic Rocket Forces, then to the return of warhead from deployed to non-deployed status, and ending with the transfer of the warhead to a disassembly facility. If a warhead is re-manufactured and re-assembled, it would be accounted for as a new warhead once it is turned over to the respective Ministry of Defense or Department of Defense.

Every piece of equipment that supports warheads in each country's warhead operational system is dedicated, certified, and continuously protected within secure facilities and storage sites. All handling and transportation functions are conducted under strict, pre-planned procedures within the overall warhead operational system. New equipment must be thoroughly checked and certified to meet warhead handling standards before it can be introduced into the system, where it is secured, tracked, and accounted for during its entire service life. During CTR nuclear security cooperation, all equipment was x-rayed, and all software was examined for bugs and backdoors before being deployed to operational sites. All warhead logistics require dedicated, certified, and secure handling and transportation systems, including cranes; forklifts; gurneys; and associated handling and lifting gear; cargo trucks, cargo railcars, and guard force railcars. While air transportation systems may conduct dual-use operations, when they are used to ship warheads, they are examined and certified for nuclear warhead operations as well. Even when all this support equipment is not in use, it is secured within the closed warhead operational system.

Through previous experience with the CTR nuclear security cooperation program, we also know that each side monitors and tracks the location, status, and usage of all support equipment, transportation systems, as well as the identification of personnel, within this closed system, using dedicated inventory control and management systems. Through technical exchanges with China on the Nuclear Security Training Center conducted by DOE, we also know that China has a robust inventory management and accounting system. Thus, all this data regarding systems within the closed warhead system is already being collected on a continuous basis and maintained at least for the duration of the life cycle of the individual warheads and support equipment, and thus can be relevant in developing verification measures for a future agreement addressing warheads.

Within this closed system, all warhead movements and transportation routes must be pre-planned, approved, and secured. All storage locations, even temporary stops between locations, are approved and continuously secured. While it may seem that warheads may be located anywhere within a country or in the world, because the locations and routes cover such large areas, if one considers that security concerns do not permit warhead movements to make unplanned or unsanctioned stops along the transportation routes the closed system is not as expansive as it might appear. In fact, under a future negotiated agreement, the closed systems can be defined, declared, and "mapped" to define their boundaries for purposes of the agreement and its verification mechanism.

In Figure 3 below, a representative map shows the areas in blue associated with all Russian warhead storage sites and the facilities where warheads are first assembled and later disassembled at the end of their life cycle. As one can see, the defined areas within the closed system are limited to a relatively small, well-defined, and relatively permanent area within the country.

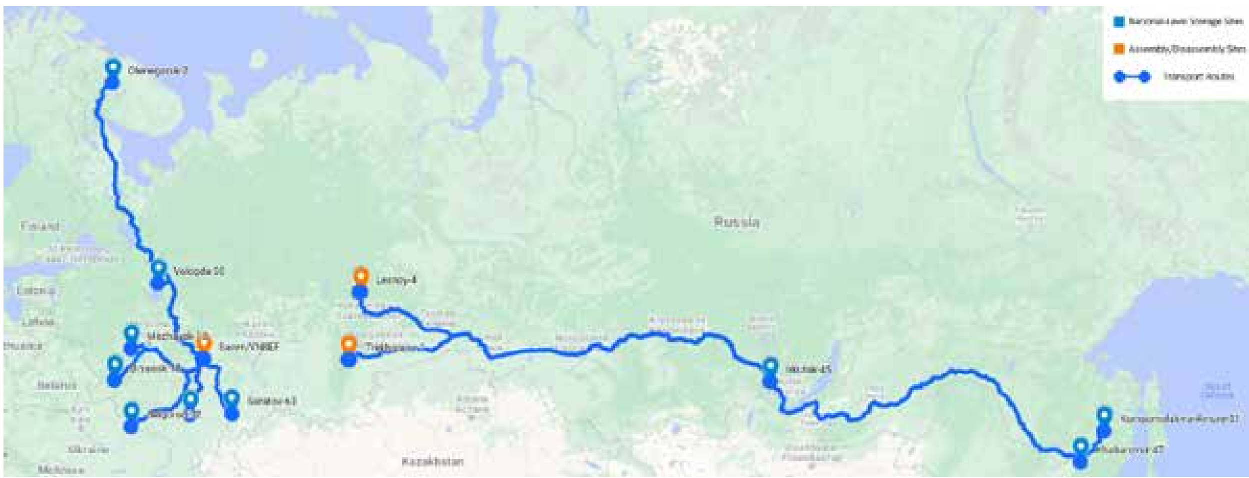

Figure 3: Russian warhead closed system for central storage sites and assembly/disassembly facilities. The map is accessible here: https://www.google.com/maps/d/u/0/edit?mid=1RLx-Q94vJDoPUpfA1oWbzPlkRPJpl-4&usp=sharing.

In Figure 4 below, a representative map has been drawn to define the closed system associated with one of the central storage sites (Bryansk-18) in Russia. The warhead operational system for each central storage area can be mapped in a similar fashion, showing the limited areas where such operations are conducted and can be defined as closed system under a future agreement addressing warheads.

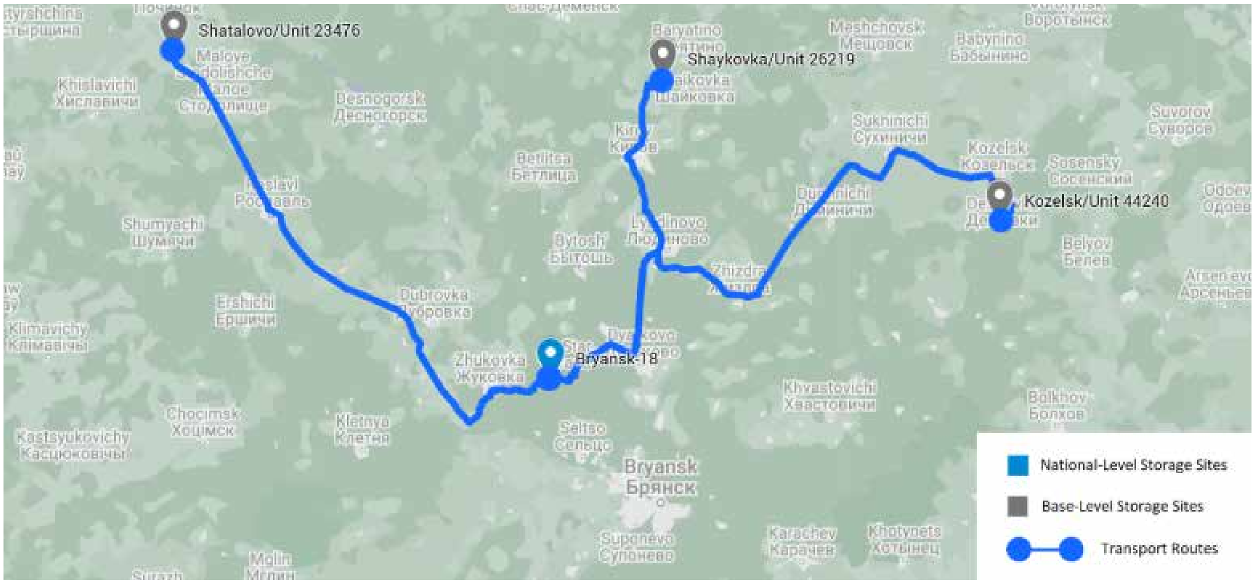

Figure 4: Bryansk-18 Central Storage site and associated sites containing bunkers for warhead storage facilities at other military bases. The map is accessible here: https://www.google.com/maps/d/u/0/edit?mid=1kUkC9aATsitZGWORZJ7xf1QtcioljvE&usp=sharing.

As these figures depict, the closed warhead operational system covers a narrow system of arteries and major depots rather than a broad and considerable amount of territory. These closed systems are closely monitored by both countries, primarily through NTMs, and are well-defined and understood.

The first step in developing a menu of verification measures, therefore, involves a declaration of the locations, allowable transportation areas, and dedicated transportation and handling equipment that make up each country's warhead operational system.

A. PROCESS FOR WARHEADS TO ENTER AND EXIT A CLOSED SYSTEM

As CNS described in our demonstration of the WTS, warheads are added to the database when they are transferred from the custody of the Department of Energy (DOE) to the Department of Defense (DoD) in the US and from the custody of the Ministry of Atomic Energy (Rosatom) to the Ministry of Defense (MOD) in Russia. The date and time of the transfer of custody becomes the first entry in the warhead passport. When a warhead reaches the end of its lifecycle, the same process in reverse would record its exit. The last entry in the passport would be the transfer of custody to DOE or Rosatom. Once again, this would apply even if a warhead is re-manufactured. It will be accounted for as a new warhead if/when it is transferred back.

We also need to consider when warheads enter and exit the closed system by transfer to a deployment base. In Russia, any transfer of a warhead from a storage bunker controlled by the 12th Main Directorate (12th GUMO) to one of the military services would be a transfer out of the closed warhead operational system. For the US and Russia, exits from the closed systems would include transfers from bunkers to be installed on ICBMs, transfers to the Navy for deployment on submarines, and removal of an ALCM or gravity bomb from a bunker and transferred to the crew responsible for installing the weapon on an aircraft such as a bomber, or on any other delivery vehicles or platforms. For the purposes of this paper, the warhead is considered leaving the closed system once it passes from the service charged with maintaining the warheads in storage to the crews of a warfighting Service. Given that both the US and Russia have declared that all their warheads designed for tactical range systems are stored in central storage bunkers, none of those warheads should exit the closed warhead operational system until they are removed from service.

B. USING SENSORS ON SUPPORT EQUIPMENT AND FACILITY INFRASTRUCTURE TO ENCLOSE WARHEADS WITHIN THEIR CLOSED SYSTEM

Having defined the concept of a closed warhead operational system, the next step in developing a menu of verification measures is to identify ways to ensure in a verifiable manner that the system remains closed, and all warheads are contained within it. Since it would be a safety and security violation to attach any kind of sensors directly on warheads, another way to achieve this objective is to place sensors on all the handling, transportation, and support equipment and on the appropriate gates, entry ways, and nuclear security equipment at temporary and permanent storage facilities. Sensors on the applicable handling equipment and transportation systems would record the opening of any doors when the warhead is loaded, and sensors could also be installed in the transportation system to record the loading as well. Sensors on the transportation and handling equipment would also record the time, date, and route of the shipment and the opening of doors and measurements of the presence or absence of a warhead in the transport vehicle or railcar. Thus the data collected by such sensors will be matched by corresponding data to be recorded in each warhead passport.

The key concept of this verification approach is that nuclear warheads cannot exist safely and securely outside the closed system without specialized support equipment. Either side would need a truck or train, or at least a gurney or forklift, to move a nuclear warhead to any non-declared long-term storage location. The warheads would need extra security if they were moved to a non-controlled location – even if stored temporarily in a truck, railcar, or non-declared storage facility.

In other words, it would be difficult, if not impossible to secretly transfer warheads outside the closed system for more than a short period of time. Even one warhead would require extensive support, handling, and transportation equipment as well as a well-equipped crew that would require astronomical levels of personnel reliability to operate on its own for extended periods. Equally, if a country were to decide to create even a limited nuclear stockpile outside of any declared warhead operational infrastructure under a bilateral or multilateral verification regime, it would need to build a new closed system. Either approach would require considerable time and effort to avoid eventual detection using NTM and other tools. To address these possible violations, CNS proposes a verification regime with numerous tools and techniques to detect violations and seek clarifications of any potential misunderstandings.

The closed system approach would require the sides to agree upon location(s) or facilities where the sensors would be affixed on the newly produced support equipment to be used within the nuclear warhead operational system and where the sensors would be removed upon disposal of any equipment that reaches the end of its service life. These locations could be located outside a production and/or a certification facility. The facilities would need to be declared, and an agreed process developed to record items of interest leaving the facilities. A combination of video cameras, open display for NTM, and collection of the data represented by hash codes would be required.

These efforts would not make it impossible for the host party to produce equipment at another production facility or another certification laboratory, but it would require the host party to spend significant resources to supply non-declared support equipment. Since any warhead that existed outside the closed system would need certified lifting equipment, HVAC support, security personnel, and other support equipment if stored for more than a couple of weeks, the more difficult it would be to hide a warhead outside the closed system. The host party would need to illicitly produce handling equipment at declared or non-declared production facilities, and would need to move and store all of that equipment without ever being detected. When combined with measures to monitor warhead movements, the closed system approach provides greater chances that illicit activities would be detected by the inspecting party at some point in the lifecycle of a warhead.

Certainly, untagged support equipment that resembles similar equipment used within the warhead operation system may be in used in multiple places outside the closed system. Such locations would be strong candidates to be declared as suspect sites. In addition, the presence of support equipment at a facility that has the signature of warhead storage would call for a suspect-site inspection (see Section IV. E. Functional Verification Activities: Suspect Site Inspections).

If all support equipment is equipped with sensors that track their location throughout their service life, and other sensors are installed on fixed infrastructure egresses that serve as unmanned virtual portals, there would be no way for equipment to be used to move warheads outside the closed system without sensors detecting a violation. No certified handling equipment with sensors should ever be located outside the closed system, so, if any such sensors were identified during suspect site inspections, it would indicate a violation. It would be difficult to move equipment without sensors into the closed system and move warheads out of the closed system without risking detection by data analyses or any other type of inspection. In particular, if the closed system were to include a comprehensive virtual portal monitoring system that is recording everything going in and out of the gates at storage sites or transfer sites then there would be even more difficult to move equipment in or out of the closed system without being detected or without leaving a gap in data that is not properly accounted for. Under a closed system approach with handling, transport, and nuclear security equipment that are sensored, all movements in and out of the closed system can be recorded and correlated with additional data compiled within warhead passports and exchanged under data challenges to cryptographically protected stockpile data.

C. REQUIREMENTS FOR SENSORS

Even though the sensors proposed under the closed system approach are not attached to the warheads themselves, sensors affixed to handling, transportation, and security equipment would have to be designed so that they collect the data without transmitting it in real time or during operations – otherwise the safety, security, and reliability of the stockpile may be compromised. Therefore, the sensor would need to include strong tamper protection, and measures would need to be developed to collect the data after operations are conducted – either by conducting an on-site spot check visit of the support equipment when it is safely parked and secured in its storage area and not in use, or by the host country collecting the data and providing it to the other side by using cryptographically generated hash codes, in the same way as warhead passport data would be exchanged under the WTS methodology. Therefore, all support equipment would be equipped with non-transmitting sensors and seals to monitor their movements and activities.

If the sensors and seals are non-transmitting, there would be no way for the other side to monitor warhead locations in real time, thus protecting sensitive information. Such sensors would maintain location awareness in a way that is internal to the sensor and does not rely on external inputs and is incapable of transmitting external outputs. They would store a record of routes taken and locations over time using, for example, an inertial sensor that would only be revealed when an appropriate data reader/retrieval device is plugged in. The sensor could be installed in a sealed, black box, for example, and would reveal if the truck or other equipment deviated from a route within the closed system, thus flagging a violation. The violation would not be detected in real time but would be discovered upon interrogation of the sensor – either through a data challenge requiring the host party to reveal the data from the sensor or while collected on-site during a spot check inspection of handling and transportation equipment. It would be very important to have the sensor installed with tamper indication properties. Navigational sensors that can track routes for individual trucks or other vehicles are currently available on the open market. For example, the “Drive Right” sensor[4] pictured in Figure 5 plugs into the cigarette lighter of a vehicle and can be operated with or without GPS or Bluetooth turned on.

[4] https://www.hhdriveright.com/product-page/gm2020-temp-track

Figure 5. This navigational sensor is available from a company in the UK, and each one costs around fifty dollars. Such sensors could be used in a closed Warhead Tracking System to verify the transporation of nuclear warheads. The sensor would need further development to be tamper-proof or put in a tamper proof box on the vehicle, and some vehicular modifications might be necessary, or the sensor might need to be modified to provide its own power source. Nevertheless, even for a truck fleet of 2,000 vehicles, the total cost of the sensors would be around $100,000 plus modifications – well within arms control verification budgets.

Simple tamper-proof locking and unlocking sensors can also be installed on all doors, gates, and other openings of transport systems and facility infrastructure within the closed system to record movements in and out of any given opening. Russian warhead storage facilities, for example, are surrounded by fencing, with a main gate for entry and an emergency exit gate. Sensors emplaced on these gates could be used to record every time that gate is opened, how long it is open for, and when it is closed. Every time a vehicle transgresses these openings, the sensor captures the date, time, and duration of the opening. These simple sensors could be affixed in such a way that they act as a virtual portal around warhead storage and transfer facilities. This concept of a virtual, unmanned portal could also be extended along transportation routes by installing cameras at key locations in tamper proof protective shielding to record when transportation systems traverse certain routes and could even be used to record the speed of travel.

The arms control community has conducted significant research and development efforts on developing all sorts of tamper-proof and tamper-indicating devices to support previous arms control agreements. A recent example of current research is the work conducted by Savannah River National Laboratory (SRNL) engineers on tamper-indicating devices that was presented to the Institute of Nuclear Materials Management European Safeguards Research and Development Association (INMMERSADA) in Vienna in 2023.[5] As shown in

[5] Provided by NNSA via LinkedIn: https://www.linkedin.com/posts/national-nuclear-security-administration_inmmesarda2023-nnsa-activity-7086776843722248192-ymyV/?utm_source=share&utm_medium=member_desktop.

Figure 6 below, SRNL developed a prototype tamper-indicating device for automated robotic application that can check the serial number and integrity of a seal on a nuclear material container. Similar devices could be designed for gates, truck and railcar door locks, and other warhead handling, transportation, and infrastructure equipment. Other examples are provided in **Annex A**.

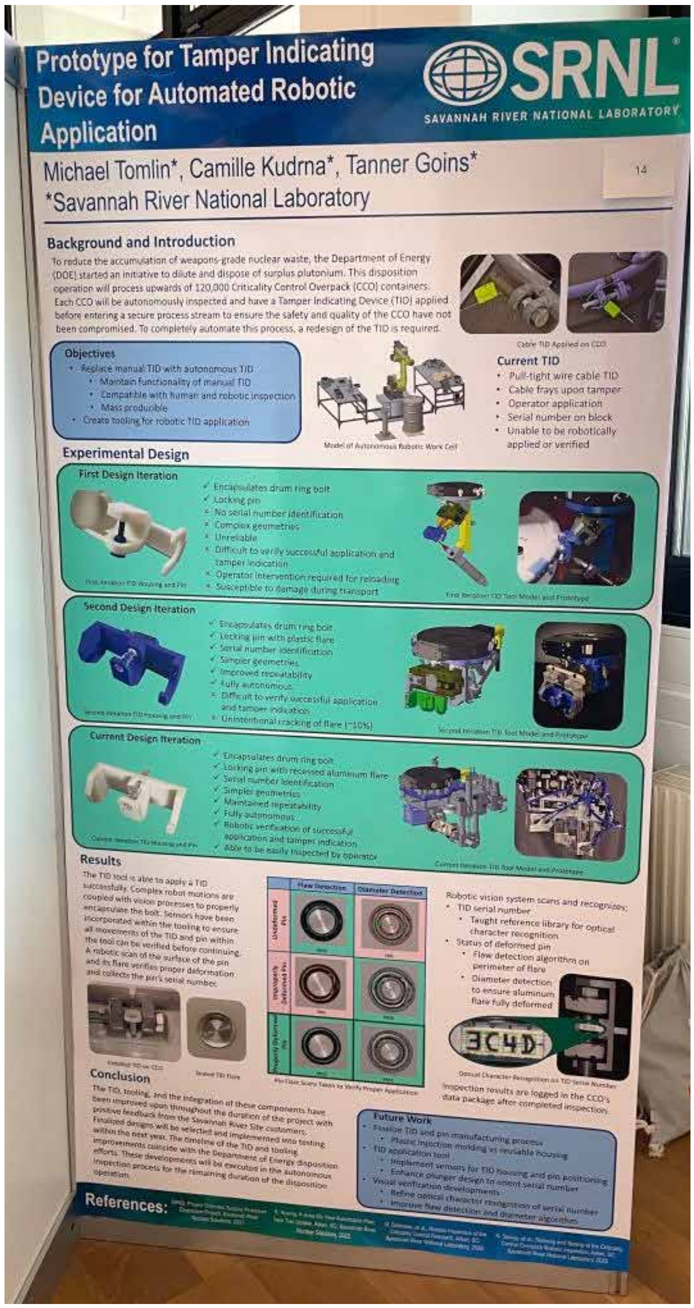

Figure 6. Prototype for Tamper-indicating Device for Automated Robotic Application. Source: Savannah River National Laboratory

Once again, the data could either be collected by an on-site inspection team through an on-site spot check visit or be collected by the host country and used to create a cryptographic hash code that could be shared with the other side on a negotiated frequency. The data could then be revealed through the same kind of data challenge process as previously described for warhead passports. With sensors installed with tamper-proof or tamper-indicating seals on all handling, transportation, and nuclear security equipment, an inspection team could collect and accumulate data on the movement and location of all declared support equipment through on-site spot check visits. That side could also obtain such information through data challenges of host-provided data in the form of cryptographically produced hash codes.

D. USING THE CONCEPT OF A CLOSED WARHEAD OPERATIONAL SYSTEM TOGETHER WITH WARHEAD PASSPORTS TO FORM THE FOUNDATION OF A VERIFICATION APPROACH

The concept of a Warhead Tracking System (WTS) previously developed by CNS provides for the development of unique identifiers for individual warheads based on life cycle logistics and operational data derived for each warhead. That data is then protected and represented by cryptographically generated hash codes. Our assumption in developing this concept is that the US DoD and Russian MOD currently monitor the locations and usage of all handling equipment within their respective inventory management systems. This is based on technical exchanges conducted under the CTR nuclear security cooperation supporting development and implementation of the Russian inventory management system.

When the data used in the passport that defines each warhead is combined with the data collected from the sensors of the handling, transportation, and nuclear security equipment used to define the closed system, a complex verification system is created that requires that all this data on warhead movements and operations matches in an integrated system. So, for every movement, data would be generated by sensors installed on all the support equipment while complementary data was being recorded and collected within each warhead passport. Every warhead passport transaction would be examined to determine whether it matched the data recorded by the relevant handling, transportation, and nuclear security equipment. And the data collected by the sensors in the closed system during every warhead movement and operation would similarly be analyzed to assess whether it matched the data recorded in the relevant warhead passport(s). Much depends on the technology of the sensor. They can be made quite difficult to tamper – it is impossible to create a 100 percent tamper proof sensor given unlimited time and effort – and even more difficult to tamper without being detected by examining data from multiple sources.

During a warhead road-to-rail transfer operation, for example, the transaction would be captured in the warhead passport indicating the date, time, and place when the warhead was transferred from the road crew to the rail crew. While that operation was taking place, the sensor in the truck would record the route taken to arrive at the rail transfer site. The sensor on the truck door would record that it was opened at a precise time – which should be consistent with the passport data - and closed immediately following its removal. An additional sensor emplaced inside the truck could also be recording data on the dates and times when the truck had a warhead loaded and when that warhead was unloaded. Handling equipment such as a forklift would have a sensor to collect data on its movements and locations as it is being used to remove the warhead from the truck and carried to the railcar. Those sensors could record the date and time of the lift and transfer. The sensors on the railcar would record when the back door was opened and when the tray was pulled out, when the warhead was affixed to the tray, when the tray was put back in place, and when the door closed, culminating the warhead transfer. For every warhead transaction there would need to be corresponding data from the sensors affixed to specific handling and transportation systems that confirm the operation within the closed system. The data analytics assessing the data integration would not be conducted in real time but could be conducted for every transaction at an agreed timeframe after the data is collected.

If a warhead were to be observed outside the closed system, then the unique identifier data previously captured for that warhead would contain either non-reported data or falsified data, or there would have been no unique identifier data exchanged at all for that warhead. Such a scenario would constitute a violation of the verification regime under an agreement addressing total warhead inventory.

As demonstrated in our previous project, developing the concept of warhead passports represented by cryptographically generated hash codes assumes that historical warhead locations and logistical data have already been exchanged between the US and Russia. If it is possible to exchange data for warheads, then it would certainly be possible to exchange data for warhead handling and transportation systems included in the overall closed warhead operational system.

Both sides are fully familiar with each other's nuclear warhead storage sites, infrastructure, and transportation routes, having conducted on site visits and exchanged transportation data under the CTR nuclear security program.[6] In fact, the CTR program provided Russia with a significant quantity of the transportation and nuclear security systems used at Russian storage sites today. All the equipment was inspected closely by both sides during the procurement, delivery, and installation procedures at neutral locations and therefore, could theoretically be examined on site at neutral locations by arms control inspectors as well. US personnel have visited almost all the Russian warhead storage facilities, and Russian technical experts have conducted on-site visits to US warhead storage facilities at F.E. Warren Air Force Base and Kings Bay, GA naval base.[7] The United States conducted a presentation of a warhead transportation convoy to the Russians at F.E. Warren, and, under CTR, US and Russian technicians designed and produced vehicles, containers, railcars, and even designed the tie-downs used for Russian warhead transportation. Russian experts have also visited the Pantex facility under an exchange program with the US Department of Energy/NNSA. The locations and support infrastructure associated with nuclear warheads are also well understood in the open-source community monitoring warheads.

[6] For security reasons, data on warheads cannot be exchanged in real time. We posited that data could not be shared until after a period of at least 30 days based on Russia's willingness to provide such data 30 days after shipments conducted under the CTR program. Transportation and handling equipment can be examined, and was examined under the CTR program on-site and in real time when not in the process of handling warheads.

7 For a first-hand account of the Russian visits and of a Russian nuclear exercise, see: https://www.stimson.org/ppl/william-m-moon/

Arms control operations for a verification protocol addressing nuclear warheads could be conducted in the same way as was done for strategic weapons sites in START I and New START. First, baseline data on support equipment would be declared, notified, and periodically validated in the closed warhead operating system. Data would also include locations and movements of trucks, railcars, gurneys, cranes, certified lifting equipment, containers, and even aircraft. Second, warhead transportation and handling equipment could be examined, and data collected from the attached sensors. Third, there could be a system of notifications about movements of support equipment, for example if certain items are moved from one site to another. Some or all the data gathered and shared between the sides on transportation and handling equipment could be exchanged in the same way as warheads under our WTS system –recorded via a cryptographic hash code. The sides would need to negotiate the extent to which data on the warhead transportation and handling equipment is exchanged or collected in its raw form or represented by cryptographic hash codes.

None of that equipment could be used to move warheads – or anything else -- outside the closed system or used to support undeclared warheads located outside the closed system. Violations would be detected through on-site spot check visits of the support equipment sensors, by examining the reported data, and correlating it with hashed warhead passport data. Any support equipment entering or exiting a secure area without being registered by seals and sensors on gates and doors of a secure area would indicate a potential violation whether going in or out of the secure area.

Over time, as more and more data from warhead passports are revealed through data challenges, and more data is collected directly through on-site spot check visits of sensors installed on handling, transportation, and nuclear security equipment, the sides will be able to correlate data involved in a particular warhead movement or operation. This process, however, need not be random or haphazard. Each side can schedule its on-site spot check visits based on the information revealed through previous data challenges, and future data challenges can be developed in accordance with the information discovered during the spot check visits. This iterative correlation of warhead passport data and information stored on support equipment sensors will increase the sides' confidence that all movements and operations are being conducted within the closed system and that there are not any non-declared warheads operating within the closed system nor any support equipment moved or used outside the closed system.

Given that each side understands how the data are integrated, they can design their data challenges on warhead passport data and on their on-site spot check visits of the support equipment sensors to increase their confidence that all movements and operations are being conducted within the closed system and that there are not any non-declared warheads operating within the closed system. One important caveat to remember is that none of the data from either source would be shared in real time, so the confidence only applies to historical operations at an agreed number of days (likely at least 30 days prior, if not longer). This delay represents, in our view, an acceptable compromise between the sensitivity of real-time data and the need to build verifiable trust as well as a reasonable probability of detecting and reacting to potential violations.

The amount of data that could be subject to collection and compilation could be quite extensive considering warhead passport data and all the associated support equipment such as the lifting equipment, cranes, gurneys, tie-downs, trucks, railcars, aircraft, or any other equipment involved in warhead operations. Clearly, the parties to any agreement would need to negotiate how much of that data would be subject to collection and how much would be subject to data challenges. Based on previous CTR exchanges, however, we know that all such data is being gathered and collected by existing inventory management systems and does not require either side to create new data. The closed warhead operational system ensures that allowable activities within the system can be tracked, validated, and verified.

E. USING A ZK-SNARK TOOL TO CONDUCT ANALYTICS ON DATA COLLECTED FROM TRANSPORTATION AND HANDLING EQUIPMENT REQUIRED TO SUPPORT EVERY TRANSACTION IN ALL WARHEAD PASSPORTS

There are two ways to integrate and compare data collected by sensors on transportation, handling, and nuclear security equipment with data compiled in the warhead passports used as unique identifiers for each warhead. The data can be collected through data challenges issued for one or both sets of data, in which case the revealed data can be examined by the challenging side and compared to confirm consistencies and identify any anomalies.

The second way to conduct the data analytics would be to use a zk-SNARK (Zero Knowledge Succinct Non-Interactive Argument of Knowledge) tool like the one CNS developed and demonstrated alongside the WTS in December 2022. This tool allows an inspecting party to assess the integrity of warhead passport data without revealing the data itself. It can directly interrogate the data that was used to generate a representative hash code and confirm for the other party whether the data has been compiled in accordance with rules specified by the two parties. In this case, the tool would need to be programmed to assess the integration of data from the warhead passports and from the sensors on the transportation, handling, and nuclear security equipment to see that every relevant warhead operation can be confirmed by transactions recorded in the warhead passport and all equipment used in that specific transaction. This can all be done without any of the data being revealed to the other side, but if done on a regular and sustained basis, it can confirm that all the data that is being collected follows the rules in place for all warhead operations.

F. CORROBORATING AND CROSS-REFERENCING WARHEAD PASSPORT DATA AND SUPPORT EQUIPMENT HANDLING DATA

Utilizing our closed system concept that would entail placing sensors on all handling, transportation, and nuclear security systems, there would not be any warhead operation that could be conducted without generating data that would be collected by multiple sensors and without generating an additional, complementary transaction captured within the warhead passport. Even a routine security check would generate data collected by a sensor on the gate or doorway leading into the bunker where the warhead is stored, and that operation would generate a complementary or matching transaction within the warhead passport. All warhead operations, therefore, would produce one or more transactions that make up the warhead passport which would require corroborating data collected by transport, handling, or nuclear security equipment contained within the closed warhead operational system. Under this verification concept, two sets of data on all transactions conducted on warheads would be captured and available to corroborate -- either by a manual examination of revealed data or by a validation check conducted by a zk-SNARK tool on the data represented by hash codes. Even if very little data has been revealed, the sides would gain confidence in the validity of the data representing the applicable warhead stockpiles through data analytics, and the confidence level would increase further over time as more data are revealed, correlated, and corroborated. Data challenges and random on-site spot check visits could then be designed to increase confidence even further.

This system would greatly deter cheating because it would require either that false data be entered into both the handling systems and the warhead passports, or that data be omitted from both. In the latter case, a void of data would be detected through the logic checks conducted by the zk-SNARK that could be followed up with specific data challenges. With such strong controls and data collection within the closed system, and in detecting and collecting data on all warheads and handling equipment entering or exiting the closed system, the difficulty for either side to maintain an inventory of non-reported warheads would increase. Any equipment with sensors detected at non-sanctioned locations through suspect site inspections would constitute a violation, as would the presence of any related warhead. It would be quite difficult for either side to move declared warheads and/or declared support equipment outside of the closed system without violating the provisions that govern allowable warhead operations, movements, and locations in a future agreement.

With these measures in place, non-declared sites and activities required to support non-declared warheads can be more easily spotted and identified, because violations could be detected not only by spotting and identifying a suspect warhead, but also by identifying declared support equipment in a non-declared location or undeclared support equipment at a suspect site capable of supporting non-declared warheads. Thus, no declared equipment could be used to move warheads outside the closed system or used to support undeclared warheads located outside the closed system without being detected by sensors on entry/exit points or by on-site spot check visits of the support equipment locations. The on-site spot checks could include gathering data from the sensors and combined with a data challenge procedure to reveal data from relevant warhead passport(s) that together would increase confidence that no unauthorized equipment or warheads have been moved in or out of the closed system. By using these measures together, the verification regime would make it difficult to move either support equipment or warheads in or out of the closed system. Once a comprehensive closed system is established and operating, a country would have to develop and operate a non-declared warhead production facility and develop outside production facilities for all required handling, transportation, and nuclear security equipment in order to maintain a stockpile of non-declared warheads outside the closed system. It would also require them to maintain highly reliable, separate security forces to sustain any number of warheads completely outside the closed system.

To mitigate the risk of warheads and support equipment all produced and maintained outside the closed system without detection, CNS proposes that the sides consider the possibility of using additional sensors at other sites, such as conventional weapons storage sites, that would be declared suspect sites. This smaller set of sensors would help detect the illegal presence of nuclear warheads at any suspect site that might possess capabilities like nuclear warhead handling, transportation, and security equipment. This measure would further narrow the options available to circumvent a closed system verification regime and thus enhance the capabilities of traditional suspect site verification measures to detect any potential oasis containing all the required support, handling, transport, and nuclear security capabilities and warheads. These measures will be explained further in the suspect site inspection section later in this paper.

IV. Menu of Verification Technologies, Devices, Measures, and Procedures

Using the cryptographic techniques that CNS developed to support data exchanges on warheads, it would be possible to pursue traditional arms control measures such as have been used for START and New START. In order to increase confidence for an arms control regime addressing warheads without violating security and safety concerns, we offer an alternative closed system concept for consideration. Instead of seeking methods to identify warheads based on their composition, this approach would help verify declarations by closely monitoring support, handling, and nuclear security equipment used within warhead operations together with data from warhead passports.

For this approach, our menu of verification technologies, devices, measures, and procedures has been organized into five functional categories tied to the operation of this closed operational warhead system: A) Functional Verification Activities Establishing a Closed Warhead Operational System; B) Functional Verification Activities Monitoring Containers, Trucks, Railcars, Aircraft, and Nuclear Security Systems; C) Functional Verification Activities: On-Site Visits/Challenges at Declared Facilities; D) Functional Verification Activities: Displays and Close-Outs; and E) Functional Verification Activities: Suspect Sites.

Within each of these functional categories, we have identified the verification activity itself, the verification targets, the goal of this verification measure, the techniques and technologies that can be used, and the negotiability and procedural and technical precedents of the functions, techniques, and technologies identified. We address and describe the intrusiveness of the techniques and technologies in each section as well.

A. FUNCTIONAL VERIFICATION ACTIVITIES ESTABLISHING A CLOSED WARHEAD OPERATIONAL SYSTEM

Once the sides declare all the locations, including allowable travel corridors, that constitute the closed warhead operational system, the next step would be to install sensors on all applicable transport, handling, and nuclear security equipment that would be operated within the system. These sensors act together to function as a virtual, unattended portal monitoring system. One important point, however, is that none of these sensors would have the capability to transmit data. While the ability to transmit data would increase confidence in the integrity of the closed system in real time, such a capability, if realized, would pose an unacceptable security violation and create security vulnerabilities for both sides.

Our proposed approach would involve sensors that collect relevant data to establish and maintain the closed system and would use cryptography to protect the data until the sides agree to share some of the data through negotiated data challenges and on-site spot check visits to collect data from the sensors at neutral, allowable locations at least 30 days after the last operation has been completed. That is why all of the sensors we are proposing for handling, transport, and nuclear security equipment will require robust seals that record the data and time of any use of the applicable equipment.

The targets of these functional verification activities include all transport, handling, and nuclear security systems within the closed system. All doors and gates where warheads could pass through would be equipped with sensors that record every time they are opened, how long they are opened, and when they are closed. All transport equipment would be equipped with sensors that measure the routes they traverse and the dates and times of all movements. As described above in our explanation of our verification concept, these sensors would not function with GPS but with inertial technologies and would not include capabilities to transmit the data off-site. The doors and openings of these transportation systems would also be equipped with sensors identifying the times and locations where they have sensors to record when the equipment was used and what function it performed. The sides would negotiate which containers would be equipped with sensors as well. Sensors on containers may be more sensitive than sensors on other support and handling equipment, so if a comprehensive agreement on all other equipment can be negotiated, the side may want to forego attaching a sensor to a container with a warhead inside it since that may pose safety or security concerns, but any containers that may be used during transportation, or that are located in the closed system for any time that they do not contain a warhead, would need to be sealed with a sensor that identifies when the seal is in place and what times it was broken in order to conduct a specified operation.

Even when support equipment must be moved to a maintenance facility, for example, the verification regime should include a protocol to declare such facilities and enable the closed system to account for movements to and from such facilities.

The process of establishing and maintaining the closed system would not require particularly intrusive techniques and technologies. Under our closed system approach, the sensors would be affixed or installed when the transportation systems are not in use and this process would be accomplished at their secure parking areas or at nearby neutral, non-sensitive areas. This would require the inspecting team to send an installation team in-country, but they would go to locations where arrangements for US or Russian personnel can be made as was demonstrated during the implementation of nuclear security cooperation under the CTR agreement. None of the technologies we have identified would include the capability to transmit data off-site, and all the data collected by the sensors could be protected by generating hash codes to represent the data until such time that the sides agree to disclose that data.

Installation of sensors on handling and lifting equipment would be more intrusive – at least for those systems used within bunkers. It would not be too difficult or disruptive to move forklifts to a secure parking area nearby, but that could be problematic for some cranes, and especially for cranes inside bunkers. For such cases, the sides would need to determine the necessity for placing seals or sensors on non-mobile cranes.

As shown in Table 1, our menu includes other sensors that would be considered more intrusive than the simple seals and route measuring devices described so far. These include cosmic ray and thermal neutron sensors that could be installed inside transportation systems such as trucks and railcars to detect and record when warheads are inside the cargo area. Weigh scales are another possible sensor that could be used within transportation vehicles such as trucks or railcars. Sensors intended to detect and potentially count warheads are more intrusive, expensive, and complex than tags and seals on doors and lifting equipment, and there could be concern from the host country that the sensors could gather sensitive data. While they would be designed and calibrated in such a way that they would not measure or collect sensitive data on the composition or design of any warheads, they could be calibrated to not only detect the presence of a warhead, but also to count the number of distinct warheads within the cargo space. These types of technologies would provide a greater level of confidence in the verification system than more simple seals and sensors attached to the tie-downs inside the transportation system's cargo space, but they would be much more intrusive. We looked at potential technologies that might also be used to detect whether a nuclear warhead was recently inside a specific cargo area, but the technology required for such readings would be even more intrusive and would not greatly increase verification confidence under our approach.

We also included a quantum tracker in our menu. This is a more advanced technology and may be considered even more intrusive and difficult to negotiate because it is not as well understood and could create hesitancy in gaining acceptance, but quantum technologies can be used to enhance the confidence in seals and route measuring devices and may not involve significant cost increases. We assess that quantum technologies could be a future enhancement to verification technologies and techniques that should be considered at a later stage in the negotiating process.

A warhead verification protocol would also need to include technologies and measures to monitor storage sites, transfer points, and production/disassembly facilities. Thinking further about the concept of a closed warhead operational system, the idea to monitor storage sites, transfer points, and production/disassembly facilities is conceptually like establishing a virtual, unmanned portal. Using similar seals on the gates and doors of these facilities can provide complementary monitoring capabilities – especially when they are correlated with the data collected from the transport systems through data exchange or through data obtained from the sensors, as well as with data contained in the warhead passports.

To be sure, with production/disassembly facilities it may be difficult to discriminate between activity relevant to the proposed verification regime (warheads exiting or entering the facility) and other activities involving the opening of the gate(s). Such a system may be deemed excessively intrusive by Russia if they perceive the US proposal provides information outside the purview of the agreement.

When it comes to nuclear warhead storage sites, however, it is useful to analyze the details associated with the security systems that surround them. These details are well known based upon years of nuclear security cooperation between the US and Russia under the CTR program, to include joint design of the security systems at Russian sites and Russian visits to US based bunkers at FE Warren AFB and the Kings Bay, GA Naval base. The fencing around the bunkers for US and Russian warhead storage sites each have two entrance points, but one is typically used only for emergencies. Therefore, it may be possible to apply a seal on the emergency exit that would indicate any intrusion, and another one at the main entrance that could be used to indicate when and how often the gate was opened. Under the least possible level of intrusiveness, the data could be entered by the host country and represented by hash codes that could be challenged by the other side at later, random dates. A medium level of intrusiveness could involve the use of video to permit the other side to have a visual record of the representatives of the host country collecting and entering the data without hash codes. The most intrusive approach would involve an on-site spot check visit to the bunkers where the inspection team would collect the data from the sensors during the visit. The sensors would need to be tamper-proof and able to detect any tampering or hacking capability.

Since NTM is already being used to monitor these sites, NTM data could be correlated with data collected from the sensors, which would enhance confidence in the validity of data on activities at these sites to a level higher than it is today.

Based on our CTR knowledge and experience, we also know that both sides use radiation detection sensors at the entrances to the bunker sites. From a nuclear security perspective these are used primarily to ensure there is not an unauthorized exit of radiological material from the site when certain vehicles exit. Personnel exit sites through special personnel gates that do not permit larger objects to pass through. It would be slightly more intrusive for the sides to exchange data that is already being collected from these sensors, but by doing so such data would provide an additional layer of confidence in the validity of the reported data. For an even higher confidence level, the sides could also add a sensor reader to the gate system that would be used to identify, and perhaps take a video or picture, of every vehicle that passes through the gate. We know that the security systems already monitor, gather, and store such video data, and such data could be shared at an agreed date and time after such an operation is conducted. If this were combined with another sensor to record the serial number of each vehicle passing through the gate, read at the gate by a permanently affixed serial number or bar code, then there would also be a record of every time the gates were opened. That record could be analyzed to determine whether it corresponded with the movement of a vehicle that transported a warhead in or out of the facility. Such a procedure would require the collection of data on all traffic transiting the gate.

The security systems at the Russian Rail Transfer Points (RTPs) are designed in a similar way as those at permanent storage sites. These security systems were also jointly developed and implemented under the CTR nuclear security cooperation program. In this case, each railcar that transited through each gate would be recorded and the data would be collected to indicate whether it was loaded or unloaded (corroborated by warhead passport data).

For an even more intrusive menu, advanced radiation techniques could be employed that not only identify whether a truck or railcar was empty or loaded when it passed through the gate, but that could also identify the number, type, or even individual warhead(s) involved in the movement.

All the techniques and technologies we have identified to perform the function of establishing a closed warhead operational system are based on successfully implemented precedents that indicate that such measures have a high potential of negotiability. If a political/military environment exists that would be conducive to technical discussions on an agreement addressing warheads, our analysis and menu have identified an approach to establishing a closed system with techniques and technologies that offer opportunities for a potential agreement.

Table 1. Functional Verification Activities Establishing the Closed System

Function	Target	Goal	Techniques & Technologies	Negotiability/Precedents
Unattended portal monitoring – data collected via data challenges and/or on-site challenge inspections	-Gate(s) installed at key road/rail points (inspecting party observes installation and records unique identifier for each) -Virtual portals – storage facility, rail/ air transfer point, production/ elimination facilities	-Data recorded by host, then gathered by inspection team on site at designated times/ locations -Sensors on gates record every time gate is lifted and unique identifiers of all trucks/ railcars passing through are recorded by host party. -Pictures/video with date/time stamp correlated with unique identifiers on trucks/railcars. -Confirm declarations / notifications. -Confirm that only declared trucks/railcars are allowed to pass the gate. -Absence of non-declared warheads.	-Gates at key road/rail points such as bunker entrances, production facility entrances/ exits, transfer points -Cryptographic development and capturing of hash codes - Cosmic rays 2 sided, counting highly dense objects going in/out - Thermal neutron counting (high probability to be acceptable) - Neutron multiplicity - Spectroscopic gamma ray imaging - NMIS/FNMIS - Quantum tracker (Q-ID)	-CTR: visited storage sites and went to the gates, installed radiation detectors at entrances -INF, START I: portal monitoring procedures and equipment -DOE, US-Russia initiatives, US-UK Verification, NuDiVe: various portal monitors
Inspecting party observes as host installs sensors on cargo trucks, railcars, aircraft, and containers (and handling equipment, if agreed)	Cargo railcars, transport trucks, aircraft & containers	-Confirm installation of sensors and record each sensor's unique identification code and association with unique container, truck, railcar, or aircraft	-Cryptographic development and capturing of hash codes identifying each unique item. -door seals that record and measure opening and closing of doors -sensors attached to tie-downs to record presence of container, size or weight range for container loaded or unloaded	-UKNI, US-UK: tamper-indicating seals -Open Skies: hashing software -START I, New START: inspection procedures, seals

B. FUNCTIONAL VERIFICATION ACTIVITIES MONITORING CONTAINERS, TRUCKS, RAILCARS, AIRCRAFT

Under our concept of a closed warhead operational system, there are several verification technologies and measures that can be used to record data on warhead handling, transportation, and nuclear security system operations. Although we use the word "monitoring" to describe our verification function, it would be more precise to note that the sensors are monitoring the movements, and the sensor data would be collected by an inspection team during each on-site spot check visit and would also be obtained through data challenges, and thus the data would not be obtained in real time or on a continuous basis.

The first challenge is to obtain data concerning the movements of all this equipment to ensure it stays within the closed system (including maintenance and repair facilities) and that records the history of the routes followed for each of their movements. Non-transmitting route capturing sensors such as the “Drive Right” system described above would be the least intrusive of the technologies and devices that could be used. While the technology exists and there are some devices available off-the-shelf, fully operational devices that would be required to fulfill this mission would need further development in the arms control R&D community. Improved devices exist but would require their own power source and would need to be either tamper proof or tamper detectable. The sides would also want to make sure that these devices are not capable of transmitting data and cannot be hacked. Design work would also be required for installation of sensors on any/all transport systems and handling equipment that the sides would agree to monitor. These could include everything from trucks and railcars to gurneys, cranes, and mobile lifting equipment. Air transport planes and helicopters could be included in this category as well if the sides agree to include these transport systems.

The data from the sensors could be gathered by the host country and recorded via a cryptographic hash code that can be shared with the other side, or data could be gathered by the inspection team during a spot check visit to a site where the support equipment is located. The latter is more intrusive and therefore would likely be subject to limits on the number of such visits per year.

The sensors and/or seals installed on the doors on the transport systems to establish and maintain the closed system (described above) should also collect data on the date and time when they are opened and closed, which will indicate when warheads are being loaded or unloaded. Such seals can be designed to record the date/time of every opening and closing. The technology for such seals exists off-the-shelf, but again it would need further design and application work to affix it onto the specific vehicular doors. In addition to seals on doors, it may also be possible to affix such seals on warhead tie-downs that secure the warhead container to the transport mechanism. During CTR cooperation on nuclear security, the US and Russia held technical discussions and jointly designed and produced tie downs for supercontainers that were provided to Russia for warhead transportation and storage, so there is precedent for tie downs that would not be overly intrusive.

Other technologies and techniques identified above to establish and maintain the closed system could also be used to record data on the loading and unloading of warheads on transportation systems. Within trucks and railcars for instance, an inspection team could use a detector to measure potential emanations from warheads that would indicate that a warhead was loaded in the vehicle within a certain amount of time. Such an approach to recording data on loading and unloading warheads could be simplified if certain seals were affixed to warhead containers that would be “read” or detected by a bar code reader installed in the transportation system, but we have not included these in our menu because we believe the sides would not allow any type of seal to be placed directly on a warhead container. Under the Warhead Safety and Security Exchange (WSSX) program, US and Russian teams worked together on developing a system that could detect the movement or removal of a warhead from a storage bunker. The Russian team strongly opposed any methodology that would directly affix a technology or sensor directly on a warhead or its container. Instead, together they developed a system of wires that would closely surround the warhead in its container that would achieve that objective without physically touching the warhead or container. If current warheads and monitoring technologies were able to overcome these earlier safety objections and the sides were to agree on such a level of intrusiveness, then using such a technology would provide a simpler solution.

Our menu includes technologies and techniques that could be placed at specific locations along designated routes. These technologies and techniques would be relatively simple, such as using NTM or placing video or still cameras but would be considered more intrusive if their placement were to reveal sensitive information on transportation routes. In our description of the closed system concept, we noted that the sides would need to identify transportation corridors in their initial declaration. This could be accomplished by simply identifying the origin and end points in the system, but such a declaration may not be sufficient for the sides to accept. If the sides were able to agree upon one or more locations along designated routes, this would increase verification confidence and would enable the use of video or still cameras to be installed at such locations to record truck, rail, or even air shipments passing through the specified egress. Drones and scintillator fibers installed at these locations could perform similar functions of gathering data on transportation systems movements. Theoretically, drones could be used to follow transportation movements, but this would likely be too intrusive given that drone movements may increase capabilities to track movements in real time using NTM and we discarded this technology from the design of our verification regime. In addition, drones would be providing a duplicative function to internally installed transportation monitors using inertial technologies. These concerns would need to be alleviated during negotiations before drone technologies could be considered as an alternative to a specific on-site inspection.

If the sides were to agree to record transportation systems movements by agreeing to install sensors at one or more designated locations along routes, it would be relatively easy to identify the appropriate technology or technologies to be used to record the data. A reader could be installed at the neutral location and another sensor could be applied to all relevant transportation systems within the closed system. These could be simple bar code readers, for example, or another non-transmissible technology.

While internally installed inertial route recording sensors would provide basic data on movements within the closed system, additional sensors that could be placed along routes within declared transportation corridors would provide an additional level of verification confidence in the integrity of the closed system. In that case, data could be collected and analyzed from three separate sources: inside the transportation system, from sensors along a route, and in the warhead passport. As more of this data is revealed via data challenges or on-site spot check, or if it is analyzed by a zk-SNARK tool, the corroboration of data from three sources would greatly increase confidence in the collected data.

Table 2 below identifies these techniques and technologies as well as the applicable precedents for each of the functions. These indicate that functional verification activities to record data on movements of containers, handling equipment, and transportation systems are negotiable and offer opportunities to address warheads in a future agreement.

Table 2. Functional verification activities monitoring containers, trucks, railcars, aircraft

Function	Target	Goal	Techniques & Technologies	Negotiability/Precedents
Monitoring and tracking warhead loading/unloading on railcars, trucks, and possibly aircraft	Cargo railcars, transport trucks, aircraft	-Recording of a transfer of custody. -Unmanned sensors record data on loading/ unloading of warheads in container/railcar/ truck/ aircraft	-Seals on truck/rail/air opening door that records and measures opening/closing times. -Sensor on interior truck tie-downs that records attachment of container and weight range, (perhaps neutrons?) -Sensor data collected on-site at parking area, or remotely at nearby location, or remotely by unmanned data gathering sensors at specified locations on the route. -Neutron multiplicity -NMIS/FNMIS	-Black Sea Experiments: remote warhead verification -INF, START I, US-UK, NuDiVe 2022: portal monitoring -UKNI, US-UK: tamper-indicating seals -INF, START I, New START: transit limitations and notification requirements
Monitoring and tracking warhead movements between facilities	- Rail, truck, air shipments	-Identify & Track movements -Detect, confirm presence/ absence of warheads in trucks, railcars, and other traffic along routes. -Sensors gather data on movements that is added to WTS database by host party at designated times	-NTM -Li-6 scintillator fibers installed at designated locations along routes. -Still/video cameras at designated locations -Drones -Sensors to record declared trucks, railcars, containers as they pass by.	-CTR: vouchers for shipments of warheads designated for dismantlement -INF, START I, New START: transit limitations and notification requirements

C. FUNCTIONAL VERIFICATION ACTIVITIES: ON-SITE VISITS/ CHALLENGES AT DECLARED FACILITIES

Our third functional verification activity addresses how data would be collected by the inspection team during on-site visits given that all the technologies in our menu are non-transmitting.

From a technical perspective, there is not much difference in how data would be collected during such visits from the use of seals and sensors installed on handling, transportation, or nuclear security equipment. The functional differences have more to do with access and access procedures, so the verification activities for different kinds of locations are listed separately. This distinction will be helpful for the development of a verification protocol for an agreement addressing warheads.

All on-site spot check visits identified in this section would be conducted either on a regular periodic basis or would be scheduled in accordance with challenge procedures. While one could say that these are measures to monitor the sites, in reality they are spot checks of the sites that would include the collection of data stored in the sensors.

On-site spot check visits to declared parking areas for trucks, railcars, and other transportation modes would be much less intrusive than on-site inspections inside bunkers and US and Russian personnel have previously been invited to visit such areas during previous technical exchanges under the CTR agreement and military-to-military exchanges. Nevertheless, they would still require the host country to accept an inspection team to those areas in its country. These areas, and similar ones, have been subject to previous access visits as identified in the precedents section of the chart below. Visits to such parking areas, or a nearby neutral site if preferred by the host country, would seek first to confirm the absence of warheads within all the transportation systems cargo areas. The simplest way to do this would be visual inspection by opening all doors and entry points for the team to quickly observe inside. Rulers and measuring tapes may be the only technologies required in that case. Access to the interior of some or all the transportation systems may be required to collect data from the route sensors and seals installed inside the systems. If such access were permitted under the agreed verification regime, the sides could also consider allowing inspectors to use additional equipment such as quantum gravitometers to detect whether underground bunkers or other underground functions might exist. While the final list of equipment allowed for the inspecting party will depend on the outcome of negotiations on the provisions in the verification protocol, precedents indicate that some sort of access may be allowed to one or more of the transportation systems in their secure parking areas.

If access was not allowed to all the transportation systems, but only to one or more systems, then other more intrusive measures would be required if the doors and openings of the remaining systems in the parking area are not going to be opened for inspection. Cosmic ray detectors and ground penetrating radar devices could be used to confirm the absence of warheads in the transportation systems and could even be used to check for potential underground facilities that could hold a warhead below the parking area. Thermal neutron scanners could also be used to examine trucks, railcars, and aircraft interiors to confirm the absence of warheads as well. We consider these technologies more intrusive due to their cost, complexity, and the risk that information on other sensitive objects that may be in the secure parking areas would be revealed.

In Table 3 below, we note that one of the goals of collecting the data would be to correlate it with other data from warhead passports that has either been revealed or would be correlated by using a zk-SNARK tool.

Table 3. Functional verification activities: on-site visits/challenges at declared facilities.

Function	Target	Goal	Techniques & Technologies	Negotiability/Precedents
On-site visit/ challenge inspection at declared truck, railcar parking areas	-Warhead transport truck and railcar secure storage/parking area -Visual inspection inside open trucks and railcars	-Confirm absence of nuclear warheads and nuclear warhead components.	-Cosmic ray and/or ground penetrating radar to look for underground voids -Spectroscopic gamma ray imaging of truck, railcar, or aircraft interiors if not opened. -Thermal neutrons scan of truck, railcar, or aircraft interiors if not opened.	-INF, START I: short-notice inspection procedures -US-UK, UKNI: info barrier, radiation detection -New START: radiation detection equipment
On-site visit/ challenge inspection of sensor data from selected truck(s), or railcars at designated or other parking areas	- Rail, truck, air shipments	--Collect data from sensors on trucks or railcars -Mileage, loading/unloading, and movements -Absence of NW's and NW components.	-Visual inspection with camera recording presence/absence of all declared items -Readout of vehicle sensors' hash codes recorded into passport	-INF: inspection procedures -START I: suspect-site procedures -New START: sampling approach, RDE, inspecting launch canisters
On-site visit/ challenge inspection at declared container storage facility	Container storage facility	-Confirm absence of warheads. -Inspect seals on containers.	-Download data on gate opening sensors, on-site radiation detectors and video and/or still pictures of warheads in trucks and empty trucks entering/exiting the bunker(s)	-CTR nuclear security visits conducted at Russian and US warhead storage facilities - INF, START I, New START: inspection procedures in buildings/containers, radiation detection

D. FUNCTIONAL VERIFICATION ACTIVITIES: DISPLAYS AND CLOSE-OUTS

Open Displays

Open displays and technical characteristics displays have been a part of many previous arms control treaties and can help make significant contributions to verification of an agreement addressing warheads using our closed system approach. Open displays of warheads would probably not be permitted by either the US or Russia due to the sensitivities involved in revealing information on the composition of any warhead displayed, but more importantly because they would enable the other side to enhance their military targeting plans. Using our concept of a closed system that focuses instead on collecting data on all the handling, transportation, and nuclear security systems surrounding nuclear warhead operations, there are several ways open displays could increase verification confidence.

One way to increase confidence would be for the sides to openly display trucks, railcars, and even forklifts at designated locations and at designated dates and times. These would be considered technical characteristics displays. The display itself might not reveal much, except perhaps if the railcars were displayed with their trays pulled out, but, by recording the date and time of the display in an open manner, the other side would have specific data on the precise location of certain items. This would be helpful because that openly revealed data can be confirmed later when route data from the sensors on these items are collected and analyzed to confirm the open display. This would increase confidence in the other data that is collected by the tamper proof sensors that depict the routes and locations of the items for their recent service history. This data correlation analysis can be conducted using data revealed through other data challenges, known events, and/or by using the zk-SNARK tool if the rest of the data has not been revealed yet.

For example, the sides might agree to conduct an open display of specific on-site handling equipment such as mobile cranes removed from the bunkers, forklifts, and gurneys, and even open gates at a specific site for a designated amount of time on a specific day and time. In this way, the other side will have some data that could be checked against the data collected from those systems later during a spot check visit or data challenge. A more intrusive example of an open display would involve a train or truck that may be photographed or captured on video during a specific operation at a specific time and place. This would be more intrusive since it could impact operations. But instead, if the open display was required just after an operation was conducted, then a picture of the inside of an empty truck or railcar could also be required to be taken at the same time as the open display. Then the picture could be captured by the host party generating a hash code of the picture data at the specified time that would coincide with the time of the open display. The picture would not be shared immediately but would be subject to a data challenge at a later time.

When data from the picture and the sensors inside the truck or railcar are collected later by an on-site spot check or through a data challenge, the data from these two sources could be compared with the pictures taken by NTM during the open display. All three of these data sources would need to match given that they are each gathering data from the same operation. In this way, open displays can be helpful in gaining confidence in the other data that may be collected from the railcar or truck sensors used in the open display. In this example, the verification measures would not be very intrusive since the data from the NTM is non-intrusive, the data from the picture(s) of the truck or railcar does not require on-site presence of the inspecting party, and the data from the navigational sensors are not collected until a later on-site spot check when the truck or railcar is securely stored long after the operation was conducted. At the same time, by comparing, collating, and corroborating data from three different sources, the inspecting party gains confidence in the validity of data it is collecting throughout this verification activity.

Close-out Inspections

A close-out inspection of a former warhead storage facility or former rail or air transfer facility to confirm the absence of nuclear warheads, warhead handling equipment, and warhead transportation equipment/vehicles would not be very different under our closed system approach than what was done under previous arms control agreements. The main difference would be that under the closed system approach the challenging side would be able to use the data challenge process to reveal warhead passport information that shows the warheads previously located at the site are no longer there, and data collected by sensors on transportation and handling systems could be revealed by spot check visits or analyzed using the zk-SNARK tool to confirm that appropriate transportation shipments to remove the warheads has taken place. In addition, all relevant and negotiated handling equipment that was located at the site and had sensors installed would either be inspected on site and destroyed, sent away from the site, or would already have been transported offsite where the sensor data could be collected, and the sensors removed if the equipment was designated for elimination.

If/when a side declares that it is closing and no longer using a warhead storage facility, there are several different options available in our menu for the other side to confirm that the site has been closed.

Given that close-out inspections would not have to be different under the closed system approach than they have been in previous arms control treaties, a more detailed review of the procedures that could be conducted using data from the closed system can help demonstrate how this approach can increase confidence in the verification activity without increasing intrusiveness. Under the closed system approach, for example, a large amount of data would be collected on the warheads and operations conducted over the lifetime of a given facility. All of this data would increase the confidence level of an on-site close-out inspection, or might even make it possible for a facility close-out to be verified without requiring a site visit.

The following procedures could all be done remotely and observed via NTM:

- The host country issues a declaration of intent to close the facility. The declaration should include the site name and identifying features, the date of the removal of the last warhead, and the date of the close out inspection.
- The warhead passports for each of the warheads removed after the declaration of the closeout of the site would include d**ata on the date/time of the warhead removal** from that site that are subject to being revealed to the other side through data challenges or spot checks check visits or can be analyzed by a zk-SNARK function.
- The host country would take **photos of the truck(s) and/or train(s) leaving the facility** with the last of the warheads. The photos would be taken by the host country, converted to a hash code, and entered into the applicable warhead passports, thus making it subject to a data challenge.
- The host country would remove all nuclear warhead handling equipment, environmental controls, and all storage and transport containers capable of containing a nuclear warhead. All cranes and handling equipment including forklifts and gurneys would be removed from the site except for the crane to be used for placement of the King Tut blocks referenced below.
- An inspection team would gather data from the sensors of any/all cranes and handling equipment either on or off site, and the equipment would be disposed of in accordance with agreed procedures.

- The host country would remove all security equipment and devices within and around the nuclear storage bunkers, including all containers. All equipment should be removed from the security control room. Fencing may be left in place around the bunkers and around the perimeter of the secured weapons storage area, but all sensors, including fence disturbance systems, microwaves, and cameras should be removed from the fences and replaced with permanent, tamper-proof seals.
- The host country would take **pictures of each of the empty bunkers** after all equipment is removed and provide the **pictures** to the other side. The pictures should be used to immediately produce a hash code to verify the exact time/place of the picture taken.

The host country would transport a **"King Tut Block"**[8] to each bunker at the site and place a block at the opening of each of the bunkers. The host country would use a **mobile crane** to place the King Tut block, but the crane would be removed upon completion of the close out inspection and then be loaded on a truck or railcar and transported away from the site.

- Instead of placing a King Tut Block in front of each bunker at the site, the host country may choose to eliminate the bunkers by bulldozing or blowing up the bunkers and covering them with concrete.

All the above procedures could be carried out without requiring an on-site inspection. The compilation of data, combined with NTM, would provide a certain level of confidence that would be much higher than NTM alone. The confidence level could be increased further if the sides were to agree to more intrusive measures. So, in addition to the steps identified above, a close out inspection team would be allowed on site to view the interior of each bunker and verify that all equipment has been removed from inside the bunkers. Data gathered through the closed system approach could be further combined with limited on-site procedures such as outlined below:

- As the team inspects each bunker, the team would place a **seal on the door** when it is closed, and the inspectors would view the placement of the King Tut blocks and place a seal on them as well.
- Bunker doors would be opened and upon completion of the inspection team's inspection inside the bunker, the inspection team would instruct a representative of the host country to place the King Tut block in front of the door, where it would be affixed or sealed to the ground. The representative of the host country would take **pictures** on site that are immediately shared with the inspection team. The copies of these pictures would be captured and represented by an identical hash code and the sides would verify that they match.
- The inspection team would also place **seals on each gate** of the fencing around each storage bunker as they complete their inspection. They would also place seals on each gate entrance to the secure area within which the storage facilities/

[8] King Tut blocks are used in nuclear security as large concrete structures with heavy rebar implanted that are difficult to remove without very heavy lifting equipment and are difficult to blow apart with explosives due to the high density of rebar installed within. They are also large enough to allow easy monitoring via NTM and can be embedded with unique identifiers that could also be monitored by NTM.

storage bunkers are located. These would be tamper-proof seals that would never be permitted to be broken without conducting a follow-up inspection.

- Upon closing and sealing the **King Tut Blocks** in front of each bunker, and seals placed on any other suspect door or opening identified by the inspection team, the inspection team would seal the perimeter of the warhead storage area with a **fiber optic seal** strung through the fencing of the entire perimeter at its uppermost and lowermost heights as selected by the inspection team. Again, these would be tamper-proof seals that would not be permitted to be opened without the presence of an inspection team.

It would be possible to increase confidence even further if the sides were to agree to an even more intrusive procedure. In this case, the inspection team would be permitted to use ground penetrating radar to inspect all areas in and around the site to ensure that there are no underground storage spaces on site. If they wanted to go even further, the sides could agree to procedures like those conducted by CTR to eliminate warhead bunkers in Ukraine: removal of all equipment, filling in the bunker with concrete and dirt, removal of all security fencing, covering the former bunkers with concrete, and converting the facility back to a "green field."

Table 4. Functional verification activities: displays and close-outs

Function	Target	Goal	Techniques & Technologies	Negotiability/ Precedents
Technical characteristics exhibition (trucks/ railcars/ aircraft)	-Randomly selected truck(s) or railcar(s) at storage facilities.	-Confirm absence of warheads. -Confirm declarations / notifications.	-NTM -Doors opened for specified time period -Host party photo of each opened truck/ railcar, correlated with unique identifier for each -Verification of dimensions of equipment -Weight of equipment -Quantum tracker (Q-ID) operated by host, data posted in passport	-CTR: upgrade of trucks and railcars -INF: data exchanges, special inspections for measurement -START I, New START: exhibition procedures, RDE
Open display (warheads/ containers)	Warhead passport confirmation	-Correlate data on the display with passport	-NTM -Host Pictures captured and included in passports or database of declared items	-INF: cooperative measures -START I, New START: display procedures
Close-out inspections	- Warhead storage facility or former rail or air transfer facility	Absence of absence of nuclear warheads, nuclear warhead containers, warhead handling equipment, and warhead transportation equipment/ vehicles and to confirm transportation notifications.	-All declared items and equipment verifiably removed and cranes verifiably removed. Pictures as evidence. -Thermal neutron -Gamma ray spectroscopy & imaging random locations in facility -Hand held ground penetrating radar -King Tut blocks and seals on bunker doors -Cosmic ray to find underground voids	-INF, START I: close-out inspection procedures --US-UK, UKNI: radiation detection -IPNDV: verification of NW absence -New START: RDE procedures

E. FUNCTIONAL VERIFICATION ACTIVITIES: SUSPECT SITE INSPECTIONS

Generally speaking, a suspect-site inspection (SSI) is an on-site inspection activity at a location that has not been previously declared as containing an item limited by the particular treaty or agreement; the purpose of such an inspection is to confirm that the treaty-limited items (in this case, nuclear warheads and associated support equipment) are not located at that site. For our menu, we have also included declared conventional storage sites as subject to suspect site functional verification activities since such sites may be configured in ways similar to nuclear warhead storage sites, and may have similar handling, transportation, and nuclear security equipment. We have identified several potential observable indicators that may raise suspicions that a suspect site is an undeclared storage site. Such indicators include:

- Characteristic signatures of a nuclear warhead storage site. Characteristic features may include bunkers typical for each side and the presence of typical transportation nodes. However, the same features may be present at conventional warhead storage sites and -- at least in Russia -- nuclear warheads can be stored in temporary nuclear warhead storage sites that do not possess all these characteristics. Such temporary locations may store nuclear warheads for hours or weeks, depending on the warhead operation that may be involved.
- The presence of support equipment, such as containers like those used for nuclear warheads, vehicles, and railcars. Such equipment may be the same or similar to the equipment that can be found at storage sites for conventional warheads.

We have reviewed a number of suspect-site inspection regimes (START I, CFE, CWC, and CTBT) and, given that such equipment may be similar to the equipment that can be found at storage sites for conventional warheads, the sides should agree on the list of such equipment and clearly identify the observable features which may differentiate such equipment from similar items associated with nuclear warhead storage sites. If those features that differentiate the sites are not observable, or are difficult to observe via NTM, such sites could be declared as specific suspect sites that would be subject to a challenge on-site inspection at a specified frequency. It may also be advisable to consider other features characteristic of nuclear warhead storage sites, such as the characteristic signatures (bunkers, buildings, security systems, and transportation nodes), to help further narrow down the category of suspect sites that should be declared under the relevant agreement. This is particularly important for Russian sites that emphasize dual capability of delivery vehicles, but also applies to the United States with respect to ALCM storages and even broader if nuclear warheads are once again produced for SLCMs. In such a situation, the sides, using these and other criteria, would agree on a list of declared sites subject to SSI. Such a list could be subsequently modified (sites removed or added). Alternatively, the list could remain open – i.e., the sides would be allowed to inspect any site that fits the agreed criteria for conducting a challenge on-site inspection. Other criteria could include activities such as the arrival of certain types of railcars or transport trucks.

The sides would need to agree whether the number of SSIs would be limited per year or unlimited. Existing precedents suggest that limits on the number of SSI may be inversely related to the intrusiveness of inspections and the availability of means for resolving the issue short of an on-site inspection. Multilateral agreements (CWC, CTBT) have protections against spurious inspection requests – such requests are subject to review (approval under CTBT, denial under CWC) by the executive body. A bilateral US-Russian agreement will not have such protections to prevent misuse of SSI requests (particularly likely if there is no limit on the number of inspections) unless the sides can agree on the sites subject to SSIs or to a specific set of criteria to limit the potential sites that could be subject to SSIs. In order not to undermine the smooth functioning of the agreement, it may be advisable to allow for a two-stage procedure: the challenged side would have the right to propose alternative methods of clarifying the situation (such as provision of additional information) or to grant managed access to protect sensitive data. The equipment and procedures for this sort of on-site inspection would be contained in the agreement.

Our menu identifies various options for conducting on-site challenge inspections at declared suspect sites. Since the characteristics of the handling, transportation, nuclear security, and storage bunkers of these non-nuclear sites would be defined and agreed through negotiations, the least intrusive way to conduct such an inspection would be simply for the inspection team to examine all of the relevant equipment to verify the identified differences and to visually inspect for evidence of any sensors designated for nuclear warhead handling equipment that are present with any of the equipment at the site.

Under our closed system approach, which will include frequent analyses of all collected data (whether further released or not) by the sides and/or using the jointly developed zk-SNARK tool, the inspection team would not only be looking for warheads on the site. Inspectors would also be examining all handling, transportation, and nuclear security equipment to differentiate it from warhead-related equipment and ensure that the host country did not use any of that equipment within the closed warhead operational system. Since the sensors on the closed system equipment would record any/all such equipment entering or exiting the closed system, such an inspection would help confirm that none of the equipment at the suspect site had been used covertly in the closed system by taking sensors off sanctioned equipment and placing them on non-sanctioned equipment.

Since some US and Russian nuclear warhead operations are currently being conducted in some third-party countries, challenge on-site inspections will also have to be applicable to the territories of third parties. These may include declared and non-declared sites, so suspect site inspection procedures and equipment would have to be developed and agreed for either type of site. Declared sites should include at the very least, the NATO sites in US NATO Allies which participate in nuclear sharing, and Belarus.

The issue of third parties would also require separate agreements between the United States. and NATO member countries and other countries with a security agreement with the United States (Japan, South Korea) to allow both on-site spot check visits and suspect-site inspections in their territories. Presumably, such an agreement would be required between Russia and Belarus as well. Once agreements with their respective allies are in place, then the US and Russia would need to agree on any/all countries that may be subject to any kind of suspect site challenge inspections.

With our closed system approach that targets handling and support equipment, transportation mechanisms, and nuclear security systems, another way to address suspect sites would be to apply certain seals and sensors on key equipment at the declared suspect sites. These would be the same kinds of sensors used on warhead-related operational equipment, but instead of focusing on producing additional data on warhead operations, equipment at declared non-warhead sites would be used to provide additional assurances that no warheads have been moved in or out of those facilities. If the same kind of nuclear detection sensors that were installed at the entry points to Russian warhead storage sites through CTR cooperation were to be included, they could be used to validate that no nuclear material passed through such a portal from time of installation to the time of data collection (direct collection by an inspection team or indirect collection provided by the host country and transmitted in the form of cryptographically generated hash codes) or interrogation (by zk-SNARK tool analyses).

Further along these lines the sides could agree on placing similar seals and sensors on bunker doors that would collect data on dates, time, and duration of openings that could correspond to the host country taking pictures of loading operations for non-nuclear munitions with dates and times to enable data collection and validation showing that the bunkers were only open for those specified non-nuclear operations.

From this menu of suspect site measures and technologies, the sides could negotiate how extensively they wanted to allow such sensors to be placed on their declared non-nuclear equipment in exchange for fewer or less frequent challenge inspections. These sensors and the data collected by them would not likely obviate the need for challenge inspections, but they could increase confidence and reduce the frequency of such challenge inspections or help the inspecting team to design their data challenges and challenge inspections.

Table 5. Functional verification activities: suspect sites

Function	Target	Goal	Techniques & Technologies	Negotiability/Precedents
Suspect site challenge inspection at declared conventional storage site or non-declared site	-Non-declared site	-Absence of NW, NW components, warhead cargo trucks, railcars, containers, any designated items related to warheads.	-Inspect for evidence of sensors on any items resembling declared items - Challenge inspection (non-nuclear components) - Spectroscopic gamma ray imaging - Cosmic ray to look for voids underground and behind walls - Thermal neutron	-START I: suspect-site inspection procedures -INF: short-notice inspections, former facilities -New START: RDE, verifying empty objects, formerly declared facilities -US-UK, UKNI: RDE, managed access

F. DATA ANALYSIS CENTERS AND A MENU OF APPLICABLE FACILITIES, HARDWARE, SOFTWARE, AND COMMUNICATIONS

Until this point in the paper, we have discussed various data collection and analyses functions but have not identified the methodology for exchanging data or the facilities, hardware, software, and communications that would be needed for a comprehensive verification protocol addressing nuclear warheads. In this section we will do so.

Official exchanges of data between the parties, whether in the form of initial declarations, hash codes, or data challenge results would be transmitted and exchanged in the same manner as with all current and previous arms control agreements. Those communications and data exchanges are conducted by the US National and Nuclear Risk Reduction Center (NNRRC) and its Russian counterpart. NNRRCs can handle a higher capacity of exchanges than are currently conducted, but if the sides were to agree to an extremely high number of exchanges, the State Department may require an expansion of its facility, equipment, and personnel.

Based on our analyses and extensive discussions with experts across the arms control community, we believe that an innovative approach to arms control such as the closed system application should be implemented in a gradual, step-by-step approach that would be built by the work of joint technical teams. These teams would negotiate and agree upon the specific measures and technologies in our initial menu and other suggestions and inputs that may be proposed by other US and Russian arms control specialists and could then develop the appropriate data exchanges (and analysis). In this way, the sides would be able to plan and execute any expansion that may be required.

Depending on the progress and outcome of any step-by-step negotiations, the sides may want to consider establishing one or more joint facilities to perform specific data functions that would be required to implement a closed system approach. Such a joint data analysis center should be built or established at a neutral, third-party location. It would be required to support functions including data collection, development of one or more zk-SNARK tools, data analyses to be conducted by zk-SNARK tools, and specified hardware and facilities for generating and validating cryptographic hash codes.

The more of these functions that the sides agree to implement, the more they should consider co-developing the hardware that would be designed specifically and exclusively to manage the hash coding process and other hardware for the databases. Commercial computers could be used to perform all or some of these functions, but they all have certain operating systems already installed on them that may pose security risks to both sides. It may be more prudent to design and develop hardware specifically to perform the exact functions required and nothing else. They could also be deployed to facilities designed specifically to provide the security to perform just the functions required.

G. THE IMPACT OF NEW TECHNOLOGIES SUCH AS QUANTUM SENSING, QUANTUM CRYPTOGRAPHY, AND QUANTUM COMPUTING ON THE CLOSED SYSTEM APPROACH USING CRYPTOGRAPHY AND ZK-SNARK TOOLS

Given that the closed system approach relies heavily on the collection, deciphering, and analyses of data, concerns may arise regarding the susceptibility of these processes to technological advances in quantum sensing, quantum cryptography, and quantum computing.

Quantum sensing capabilities are already reaching or will soon enter the commercial marketplace. These may have applications to confirm the integrity of certain seals and sensors and we have addressed some of them in our menu and description of the verification regime.

During our demonstration of cryptography in December 2022, we presented and delivered a hash coding program that combined the preferred American approach to cryptography (AES) and the Russian-preferred approach (GOST) explaining that even if one side did not trust the other side's part of the code, they could rely on their own part of the code to have confidence in the protections provided by the cryptography to their data.

Quantum computing may be decades away, but during the demonstration there were questions raised about their impact on cryptography and its use under our closed system verification regime. To be sure, there are some experts that believe that quantum computers will be too hard to ever build at a scale that will break current cryptography standards. Current cryptographic commitments (as hashed declarations representing individual WTS transactions are otherwise called) can confidently be considered secure against quantum computers. Nonetheless, we would recommend that the sides employ a step-by-step approach to development where they could work together to standardize the system, negotiating and pre-planning continuous improvements in the software – all before building the initial version. Moreover, after the system is deployed, the sides would need to stay engaged to swap out parts of the program for post-quantum parts as research advances. If these developments and actions are discussed, understood, and agreed to upfront, this should not be a problem.

For efficiency reasons, the type of hash function might need to be changed to one that is specifically created to be efficient in these conditions. What this means is that it would replace the current one that combines AES (US) and GOST (Russia) so this would add another wrinkle and layer of discussions to negotiations.

Joint development of software may involve many iterations, including use of red-teaming to break draft codes before the two sides arrive at a standard both trust. Experts are currently undertaking similar efforts as they develop post-quantum cryptography. There will have to be an agreement to build in continuous improvement to address current and post-quantum cryptography challenges.

This step-by-step development approach should also be employed for the zk-SNARK tools that the sides may want to include in the verification solution. Joint development should include a pre-negotiated plan and capability to swap out the zk-SNARK programs for post-quantum alternatives in the future as needed. The current ones might be prohibitively expensive, but this is an active area of research that will need to be monitored by experts on both sides. Fully functioning quantum computers are not a problem yet and they may never become so in reality, but one needs to prepare for the possibility.

Finally, even if the sides are concerned that quantum computers may pose a future risk to data that is represented by hash codes, security of the data can be enhanced by using much larger keys. This is not a preferred solution as it slows down the system. But, if this project were to target each sides' entire warhead stockpile, it is an approach that could be considered to increase confidence in the integrity and security of the verification procedures.

The trade-off would entail additional expense. It is not clear how much additional expense may be acceptable, but this system for arms control would be used to address a small number of messages per day at the most – not billions of messages a day as would be required for a commercial solution to be offered on the internet.

This is yet another reason to consider joint development of hardware that would be solely dedicated to conducting the required functions of this arms control approach. In fact, it may be considerably more efficient to build “computers” that can run only the cryptographic and zk-SNARK programs required to support a closed system approach described in this study. It would likely operate much faster than commercial computers. We would recommend that the sides consider jointly creating hardware that transmits the cryptographic hash codes and writes the zk-SNARK proof.

H. A MENU OF POTENTIAL APPLICATIONS OR USES OF THE WTS AND CLOSED SYSTEM APPROACH TO WARHEAD VERIFICATION

The detail and novelty of the verification options proposed in this study suggest that it would be best to jointly demonstrate the concept and then build technical solutions to support various possible agreement outcomes using a “graduated” or step-by-step approach to arms control. If technical teams were allowed to discuss such a system, it could be put in place in a way that starts with some limited reporting for one type of warhead (nonstrategic, strategic, etc.), or for one or more sites, and could be expanded over time even if there was no agreement on warhead limits. The system can be tailored to monitor things like the number of actual deployed warheads vs. warheads in storage, or it could measure the quantity of an entire inventory and monitor reductions if they were agreed. With that in mind, we offer a menu of potential agreements that could begin even with small unilateral proposals that use one or more elements from these menus.

Nuclear Conflict De-escalation and De-confliction

As the Ukraine war wages on, the risk of potential escalation continues to grow. The Russians have already employed veiled and not so veiled threats of nuclear escalation to deter US and NATO support for Ukraine. One of the immediate concerns would be the fact that some Russian warhead storage sites are located within range of current hostilities. Any attack at or near such facilities, or any warhead operational movements associated with these facilities pose the risk of misunderstanding that could prompt escalatory actions on either side. Such risks could be reduced if the sides were to agree to exchange information or notifications on warhead locations and movements that could employ certain capabilities from our menus, including exchanges of hash codes on warhead numbers associated with specified sites along with updates provided over time. At the time of this writing, amid the war in Ukraine, Russia has been far less willing to provide data on relevant military sites and even ceased implementation of established New START measures, so the current opportunities for such an agreement would be quite low.

Risk Reduction Data Exchanges

Similar to, and building on, the de-escalation and de-confliction type of agreement above, the system could be used as a risk reduction initiative, designed to provide insight on the total numbers of warheads in each country. Such information could be broken down into various categories as the sides build confidence in the advantages of exchanging such numbers. For example, detailed information could be provided sufficient to specifically track data on certain warheads correlated by delivery systems. Some data could be issued unilaterally to help initiate discussions.

The 30 day or more lag in the provision of data would not necessarily provide a tripwire indicator of plans to deploy or use nuclear weapons, but unusual activity might be detected. If notifications and data exchanges were to cease, that would be an indicator of activity of concern.

Though some may view them as decreasing the value of deterrence, data exchanges could be used to bolster deterrence by sharing data on total inventory and capability. By confirming stockpile data, the credibility of the stockpile and its capability to support a nuclear response could be enhanced. They could also be used to break down definitions of the total inventory in terms of deployed, stored, scheduled for dismantlement, etc. This could be very useful to address nonstrategic warhead concerns and provide transparency.

Even if the system was only used for data exchanges, it would provide benefits in transparency and improved accountability, bolster deterrence, and demonstrate safe and secure operations.

Data exchanges could be used as a risk reduction measure to help distinguish operations on safety, security, training, and exercises from deployment and war readiness operations.

Data exchanges could also be used to demonstrate arms control progress to non-nuclear weapon state parties to the NPT.

Site Reductions or Eliminations

The system could be used to implement an agreement to reduce or eliminate warheads at one or more storage sites. If the sides wanted to reduce or close one or more sites, the system would provide data to help confirm such activities. This could be extended to include more and more sites as the sides gain confidence in the reporting and the selected verification methods.

Freeze

The system could be used to implement a freeze on overall warhead inventories (as proposed by the Trump administration and agreed to in principle by Russia) if it included a rigorous capability to monitor new warheads entering the system and old warheads as they are eliminated. The freeze could be applied to the entire inventory, a subsection of the inventory such as deployed or stored, or to one or more sites.

A freeze could be implemented using this system even if the sides do not agree to exchange data on the actual total quantities in the current inventory.

The focus of the system would be monitoring and tracking passports for warheads as they enter and exit the system. The two sides would only inspect warheads on site as they are coming in and out of the closed system. This would be like a virtual portal of production and assembly sites.

Inventory Limits, Caps, or Reductions

The system would require fairly rigorous monitoring and verification measures, in particular with regard to suspect sites, if the sides were to agree on a mutual cap on warhead inventories. Caps could be on strategic, nonstrategic, or both. Caps could be on operational warheads only, or on the entire inventory.

Support Mutual Unilateral Reductions

The system could support a unilateral initiative by either side to declare and record specific reductions or eliminations with the intent to encourage the other side to implement similar reductions. These could be applied by site, warhead type (strategic or nonstrategic), or warhead status (operational, deployed, in storage, etc.). For example, the US could use such a system to provide transparency on the warheads that it indicates are replacing outmoded warheads in Europe.

The best example of unilateral reductions conducted by the US and Russia is the 1991-92 Presidential Nuclear Initiatives (PNIs) in which both sides pledged to eliminate certain short range nuclear systems and put all warheads designed for short range systems in central storage. The initiatives helped achieve huge reductions in the sides' warhead stockpiles, but without any verification measures it was hard for either side to be confident that the other's pledges were genuine. If such initiatives were combined with non-intrusive data exchanges, however, it may be possible to reconsider unilateral reductions while providing some insight and confidence in the actions of the other side.

One side could offer to close one site in exchange for the other to close one of its sites, or a specific site. For example, it could be used to encourage Russia to remove warheads from Belgorod for safety and security reasons. It could also be used for Kaliningrad, or even to gain agreement to prohibit the storage of warheads in Belarus. If Kaliningrad is, in fact, used occasionally or sparingly for specific purposes or exercises, such a system could be developed or tailored to provide transparency to NATO on such operations, perhaps in exchange for NATO providing similar transparency regarding its warhead replacement program.

Agreement on Mutually Verifiable Reductions

If the sides were willing to pursue an agreement along the lines of the unilateral measures described above, then some additional verification measures might be considered. In order to prepare for such a possibility, even if policymakers are not considering pursuing an agreement at this time, it would still be helpful for the verification community to consider preliminary steps using some of the tools and methodologies identified in this menu with the understanding that the overall system could support verifiable reductions in the future. The closed system approach could even support such a comprehensive agreement as removing or pulling back warheads to locations further away from current borders between Russia and NATO countries.

If any of these postulated agreements were to be extended to include China, and perhaps the UK and France, it may be possible to conceive of an agreement that would seek to increase stability through a mutual agreement not to store warheads that are fully functional. There could be various ways to discuss this, starting with something like agreeing not to store fully assembled warheads. The sides could discuss storage of primary, secondary, and other components in separate locations. This data exchange process could be used to monitor components using the same methodology and selecting appropriate verification measures from the menu.

An Overall Warhead Safeguards-like Agreement

If the sides were willing to discuss allowing mutual monitoring of each other's inventories, or partial inventories, safeguards-like measures could be developed from this menu of verification technologies and processes to monitor warheads during storage. This would mean that data on handling, support, and even some nuclear security equipment may be exchanged in real, or near-real time. If it were possible to agree to such real-time exchanges, the sides could characterize the overall regime as similar in concept to nuclear safeguards, thus establishing a safeguards-like agreement for warheads. The proposed WTS and its methodology could be used to assist in monitoring and tracking movements that would greatly assist in regular reporting on the warhead inventory.

V. Conclusion

This study provides an innovative approach to support a potential future agreement or agreements addressing nuclear warheads. Using the concept of creating unique identifiers for individual warheads based on their specific service life operations, represented by cryptographic commitments, and including data challenges, this approach proposes to create a virtual, closed system of warhead-related operations that can be assessed, validated, and verified by collecting and analyzing data from a broad array of sensors deployed and installed on warhead handling, support, transportation, and nuclear security equipment. The sides can reveal data from their warhead passports to each other through the iterative data challenge process, and that data can in turn be correlated with the support sensor information they receive during on-site spot check visits. Together, these features of a comprehensive warhead verification system provide multiple layers of data that can be examined by remote analyses and on-site collection and inspection measures.

Rather than providing a prescriptive solution to the challenge of warhead verification, we provide three related menus that policymakers can draw from to support a step-by-step approach to negotiations and implementation. The first menu identifies a broad array of arms control measures and technologies that could be used to establish a closed warhead operational system for each side, and offers alternative means to both collect, assess, and validate the data associated with warhead operations. Data from handling, transportation, and nuclear security system operations can be correlated and corroborated with data from warhead passports to build confidence and understanding of warhead declarations, operations, and status. The second menu offers options to address the facilities, hardware, software, and communications requirements to support such a system, while the third menu identifies a spectrum of potential agreements that could be supported by some or all elements of the closed system approach using cryptographic warhead passports.

From these elements and approaches, a warhead verification system could potentially be developed to address an agreement on nuclear warheads. Such a system can be designed that would be both effective in developing confidence in the other side's compliance with the agreement while being less intrusive than the alternative of allowing direct observation of warheads or even direct collection of data on the composition of warheads. The menus offer more intrusive options should they be desired as well. Optimally, the sides would negotiate and design measures jointly under a step-by-step approach that would address the need to protect sensitive information and reduce intrusiveness while facilitating effective verification that produces a high level of confidence in the overall system. This methodology would increase the chances of acceptance of this set of measures and the closed operational system approach. While no approach can eliminate entirely the risk of spoofing or violations of an agreement, the ability to double and triple check data through multiple techniques would greatly increase the challenges and complexity of cheating.

For the most part, we believe a mutually acceptable solution can be designed based mostly on relatively simple and inexpensive sensors, but these would need to be deployed on a large quantity of systems. Crucially, more application R&D is required to adapt such simple commercial systems to meet the tamper-proof and data collection requirements of a closed system. Based on research we have been able to conduct thus far, this type of application R&D for these relatively simple sensors is not currently being pursued by either the NNSA or DTRA arms control R&D programs. It is important to note, however, that there is a long history of R&D on tamper proof seals that has been conducted by these programs that would contribute to any further work that may be pursued.

At the same time, the menus presented here are supported by previous arms control and technical exchange precedents as summarized in **Annex B**. The closed system approach still utilizes many traditional elements including:

National technical means (NTM). NTM could be used to support multiple functions such as observing open displays and technical demonstrations as well as being used to prompt specific data challenges to validate declared data associated with cryptologically generated warhead unique identifiers.

Tags, seals, and unique identifiers. These relatively simple sensors are key to establishing the conceptual closed warhead system approach. The menu developed here does not go into detail on all the numerous and available devices and technologies available for these types of sensors. Further application R&D and selection of the most appropriate devices would be highly dependent on the extent of the agreement and would require joint consideration. Although we did not offer it in our menu, the sides could also consider the use of "Buddy" tags[9] that would travel with warheads. These and other non-electronic, non-magnetic, and non-metallic seals and other physical unique identifiers can work in tandem with our proposed data exchange methodology.

Site diagrams. This approach, like previous arms control treaties, would use site diagrams to guide on-site inspections and would enable the inspection team to understand the layout of a particular facility to enhance its confidence with various verification activities. CNS expects that site diagrams would also be included in a verification protocol addressing warheads. In addition to its traditional uses, however, CNS envisions that site diagrams may also be used in conjunction with measures such as pictures and video that may include geo-location and date/time stamp data to support verification. The sides would need further negotiations to identify locations within facilities where pictures, videos, and other sensors or data collection devices may be located.

Pictures, video, and other data to be collected and provided by the host country. Previous arms control treaties and international agreements such as CTR have used pictures and video to enhance verification. The menus offered include such measures and identifies some of the pictures and video that would be useful, when and where they could/should be taken, and how such data would be gathered, exchanged, and collected in the warhead passport database. Pictures and video could be considered whether they are provided by the host country, taken remotely by pre-positioned cameras, or taken by remote controlled robots or robotically controlled devices. Data may be collected in real time or gathered and shared at later dates. Locations to be considered would include, for example: storage facilities

[9] See http://www.princeton.edu/~aglaser/PU127-Buddy-Tag-2017.pdf for a more detailed examination of buddy tags.

and specific areas within the storage facilities; areas within, near, or along rail, air, and sea transfer points used for transportation of warheads; areas near production/dismantlement facilities where warheads traverse. Remote sensors, including pictures and video, could also be used as a form of portal monitoring to be conducted with or without on-site inspectors.

Based on preliminary research conducted by CNS, we know that various organizations are investigating better ways to use pictures and video for verification purposes. We understand, for example, that Rob Hughes of the UK Atomic Weapons Establishment is conducting research on using cryptography to validate photographs and video. In another example, NNSA is conducting verification R&D on pictures and video capabilities that could be used in a verification protocol that reduces the previous risks associated with the tampering and spoofing of pictures and video.

The NNSA Projects include:

1. Self-Healing Encryption for Real-Time Video Authentication, a project that PNNL was contracted to begin in Fiscal year 2022.This project intends to develop a new method for video authentication using the existing Double Ratchet Algorithm (DRA), which has self-healing capabilities. The DRA uses a public-private key exchange approach which is then updated with each communication between the partners which mitigates the consequences of a key loss. This effort will study how this algorithm can be adapted to authentication, what camera and system are able to support the analysis with minimal lag, how the communication protocol is established, and how a multi-camera system would function. During the project physical single camera and multi-camera systems will be developed and tested for performance and security.

2. Multilayered Video Authentication for Treaty Inspection a project that SNL was also contracted to begin in FY22. This project seeks to develop and evaluate an authenticatable video system for monitoring under a treaty regime. The team is partnering with a commercial partner, Prometheus Security Group Global, to customize and evaluate their camera systems in the context of an inspection regime. The project will use several systems for securing the camera systems: public key cryptography, video steganography in the raw image, steganography in the compressed image, and direct analog input into the camera for scene verification. Multiple hardware and software systems will be considered, a complete system will be built, and the complete system will undergo a detailed red team evaluation. At the end of the project, a demonstrated and tested system will be available.

On-site inspections. Understanding the need to minimize on-site inspections due to their intrusiveness, their cost, and the difficulty of negotiating them, we identify a small number of key locations and associated procedures for on-site inspectors to visit to collect and confirm warhead passport and sensor data. Given the large number of storage locations in Russia, CNS recognizes that on-site inspections of all these locations may be costly, would take time, and would not be very effective except if they were specifically designed to support the validation of data that has been exchanged or gathered by other means.

Portal monitoring. While our closed system approach does not include deploying permanent inspectors to monitor activities going in and out of warhead storage sites, or even in and out of the production facilities, it does perform similar functions to portal monitoring. The key differences are the use of sensors instead of personnel and the protection of the data until or unless the sides agree to release it to the other side. CNS does not anticipate that extensive portal monitoring of warhead storage or production facilities would be acceptable to Russia or the US due to the extensive manpower and cost involved, and the relatively small value such an activity may yield. But we do think that the closed system approach could be considered using sensors and data exchanges.

Given the challenges associated with warhead verification, we believe that our closed system approach offers a fresh and innovative approach that could be negotiated with Russia and could provide relatively high confidence verification with minimally intrusive actions.

Annex A. Intrusiveness

#	Function	Non-Intrusive	Somewhat Intrusive	Intrusive	High Confidence Intrusive
1	Close-out inspection of a former warhead storage facility	NTM, warhead passports, photos of trucks and trains departing, open display of equipment, King Tut block	One on-site closeout visit; seals on doors and gates; add seals to warhead inventory; fiber optic seal on perimeter of storage area	Ground penetrating radar; thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers)	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS); dual particle gamma ray and neutron imaging systems. Assay of materials present (nuclear forensics) for evidence of neutron activation
2	Monitoring and tracking warhead movements-rail shipments	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Internal radar sensors assess rail car volume to record entries and movements. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Portal monitoring with thermal neutron and low-=resolution gamma detectors; option to use cosmic ray muon imaging; activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Portal monitoring with high resolution gamma ray detectors and active detection systems (e.g. FNMIS)
3	Monitoring and tracking warhead movements-truck shipments	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Internal radar sensors assess rail car volume to record entries and movements. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Portal monitoring with thermal neutron and low-resolution gamma detectors; option to use cosmic ray muon imaging; activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Portal monitoring with high resolution gamma ray detectors and active detection systems
4	Monitoring and tracking warhead movements – air shipments	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to WH containers	Taxi way/inspection pad with embedded thermal neutron detectors (e.g. "smart threads"); activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Taxi way/inspection pad with embedded active detection system (e.g. FNMIS)

#	Function	Non-Intrusive	Somewhat Intrusive	Intrusive	High Confidence Intrusive
1	Close-out inspection of a former warhead storage facility	NTM, warhead passports, photos of trucks and trains departing, open display of equipment, King Tut block	One on-site closeout visit; seals on doors and gates; add seals to warhead inventory; fiber optic seal on perimeter of storage area	Ground penetrating radar; thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers)	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS); dual particle gamma ray and neutron imaging systems. Assay of materials present (nuclear forensics) for evidence of neutron activation
2	Monitoring and tracking warhead movements-rail shipments	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Internal radar sensors assess rail car volume to record entries and movements. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Portal monitoring with thermal neutron and low-=resolution gamma detectors; option to use cosmic ray muon imaging; activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Portal monitoring with high resolution gamma ray detectors and active detection systems (e.g. FNMIS)
3	Monitoring and tracking warhead movements-truck shipments	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Internal radar sensors assess rail car volume to record entries and movements. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Portal monitoring with thermal neutron and low-resolution gamma detectors; option to use cosmic ray muon imaging; activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Portal monitoring with high resolution gamma ray detectors and active detection systems
4	Monitoring and tracking warhead movements – air shipments	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to WH containers	Taxi way/inspection pad with embedded thermal neutron detectors (e.g. "smart threads"); activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Taxi way/inspection pad with embedded active detection system (e.g. FNMIS)
5	Monitoring and tracking warhead movements – truck/rail transfers	NTM, warhead passports	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Internal radar sensors assess rail car volume to record entries and movements. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration.	Portal monitoring with thermal neutron and low resolution gamma detectors; option to use cosmic ray muon imaging; activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF(similar to Quantumbase's Q-ID) applied to warhead containers.	Portal monitoring with high resolution gamma ray detectors and active detection systems

6	Inspection of a suspect site declared to store conventional munitions. Also confirm the absence of warheads	NTM, smart seals on containers	Remotely monitored IR imagery with information barriers provides indication of thermal signature from radioactive materials	Ground penetrating radar; thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers)	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS). Assay of materials present (nuclear forensics) for evidence of neutron activation
7	Inspection of a suspect site not declared to store nuclear or conventional munitions. Also confirm the absence of warheads	NTM, smart seals on containers	Remotely monitored IR imagery with information barriers provides indication of thermal signature from radioactive materials	Ground penetrating radar; Thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers)	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS). Dual particle gamma ray and neutron imaging systems
8	Inspection of a warhead transport truck secure storage/parking area, including an inspection of randomly selected trucks to gather data on their mileage and movements recorded. Also confirm the absence of warheads	NTM	Sensors confirm that location data is consistent with declared routes, record that door openings are consistent with protocol. Classical or quantum PUF (similar to Quantumbase's Q-ID) appliedapplied to equipment used to verify no alteration.	Ground penetrating radar; Thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers) activation dosimeters. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers.	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS). Dual particle gamma ray and neutron imaging systems.
9	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS). Dual particle gamma ray and neutron imaging systems.	NTM, warhead passports	Remotely monitored IR imagery with information barriers provides indication of thermal signature from radioactive materials. Classical or quantum PUF(similar to Quantumbase's Q-ID)applied to equipment used to verify no alteration	Ground penetrating radar; Thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers). Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS). Dual particle gamma ray and neutron imaging systems. Assay of materials present (nuclear forensics) for evidence of neutron activation
10	Inspection of a warhead transport railcar secure storage/parking area, including an inspection of randomly selected railcars to gather data on their mileage and movements recorded. Also confirm the absence of warheads	NTM	Route data sensors confirm that movements are consistent with declared routes and protocols	Ground penetrating radar; Thermal neutron detectors; low resolution gamma ray detectors; quantum gravimeters (monitor u/g bunkers) activation dosimeters	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS). Dual particle gamma ray and neutron imaging systems. Assay of materials present (nuclear forensics) for evidence of neutron activation
11	Portal monitoring (virtual portals – storage facility, rail/air transfer point, production/elimination facilities) – to confirm declarations/notifications or to detect undeclared warheads	NTM	Sensors, imagery, and physical data (e.g. weight) provide signatures for all potential warhead containers for comparison with declared warheads. Quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Thermal neutron detection; gamma ray radiography, cosmic ray muon imaging; activation dosimeters (fission foils, U-238, Na, etc); classical or quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	Portal monitoring active detection systems (e.g. FNMIS)

#	Function	Non-Intrusive	Somewhat Intrusive	Intrusive	High Confidence Intrusive
12	Open Display of warhead or container. This could be performed in association with a transfer of custody at the beginning or end of a transportation shipment. It could also be performed randomly at negotiated times and frequency at or near a storage facility. This would be used- to confirm declarations/ notifications. The displays would be another entry into the warhead passports and could be correlated later through a data challenge	NTM, Warhead passports; visual inspection and identification of declared items	Remotely monitored visible and IR imagery with information barriers provides confirmation of declared objects and an indication of thermal signature from radioactive materials. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Thermal neutron detectors; low resolution gamma ray detectors. Classical and quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS); dual particle gamma ray and neutron imaging systems
13	Technical characteristics exhibition (warheads/ warhead containers, trucks, railcars) – to facilitate confirmation of declarations/ notifications. This could be used for example at truck or railcar storage facilities by pulling out randomly selected railcar trays to show there are no warheads in the stored areas. This could be similar to open displays, but focused on the handling and transport systems	NTM, Warhead passports; visual inspection and identification of declared items	Remotely monitored visible and IR imagery with information barriers provides confirmation of declared objects and an indication of thermal signature from radioactive materials. Classical or quantum PUF (similar to Quantumbase's Q-ID) applied to equipment used to verify no alteration	Thermal neutron detectors; low resolution gamma ray detectors; classical and quantum PUF (similar to Quantumbase's Q-ID) applied to warhead containers	High resolution gamma ray detectors, active systems with fast neutrons for imaging and signature enhancement (e.g. FNMIS); dual particle gamma ray and neutron imaging systems

Annex B. Precedents

A number of precedents, such as joint initiatives, previous arms control measures, and CTR experience, are described below, based on their applicability to specific functions and modalities identified earlier in this paper.

A. FUNCTIONAL VERIFICATION ACTIVITIES: ESTABLISHING A CLOSED WARHEAD OPERATIONAL SYSTEM

A.1. Establishment of a closed warhead operational system to enhance verification.

INF: Locational restrictions in Treaty Article VIII specify that missiles and launchers subject to the treaty must be located at deployment areas, at support facilities, or in transit.

START I: Restrictions on movements of Road and Rail Mobile launchers of ICBMs outside of designated areas are described in Article VI. Paragraph 6 of Annex J to the MOU contains requirements for the site diagrams of the designated areas for such launchers.

New START: The Treaty's Article IV similarly specifies restrictions on location and transit of strategic offensive delivery systems, while the Part Four of the NST Protocol further details the types of movements that must be declared as notifications to the other side under the treaty.

A.2. Portal monitoring – monitoring of virtual portals at storage facilities, rail/air transfer points, and production/elimination facilities to confirm declarations/notifications or to detect undeclared warheads.

INF: Continuous portal monitoring was aimed at ensuring that stages of the SS-20 were not covertly assembled under the guise of the SS-25 ICBM. Both were manufactured at Votkinsk, but the latter was not subject to the treaty. Section IX of the Protocol on Inspection specifies that only one rail line and one road within 50 meters of each other shall pass through the portal. All vehicles capable of containing a portal monitoring-targeted treaty item shall exit only through the portal, and the no more than two other exits from the site shall be monitored by appropriate sensors. Weight sensors, vehicle sensors, surveillance systems, vehicle dimensional measurement equipment, and non-damaging image producing equipment (X-ray) are installed at the portal. Any shipment that is large enough and heavy enough to contain a relevant treaty item must be declared. Depending on the declaration, the inspection procedure may include X-ray imaging and examination of the vehicle interior. Any shipment exiting the portal is subject to weighing and the measurement of dimensions.

START I: Paragraph 14 of Article XI, Section XVI of the Inspection Protocol and Annex 5 to that Protocol provide procedures related to the continuous monitoring of production facilities that may be relevant to the use of sensors on transportation means and portal monitoring of warhead-related facilities.

New START: The Treaty does not explicitly provide precedents for portal or perimeter monitoring, particularly because no production facilities may be subject to inspection under the Treaty. However, it obligates both sides to provide notifications of the exit of solid-fueled ballistic missiles from their production facilities (NST Protocol, Part Four, Section III.1), as well as outlines various procedures to confirm the conversion and elimination of strategic arms to no longer be operable or capable of carrying nuclear weapons (NST Protocol, Part Three). Depending on monitoring requirements, these procedures, including the use of tamper-proof seals and tamper-evident equipment, can be adapted for the purposes of the closed system.

Other initiatives: Portal Perimeter Continuous Monitoring (PPCM) was among the Transparency and Verification Options identified by the Department of Energy Office of Arms Control and Nonproliferation in 1996. The United States engaged Russia thereafter in the design and demonstration of portal monitors. Recent activities of Joint US-UK Verification included the development and demonstration of a Portal Monitor for Arms Control (PMAC). The Nuclear Disarmament Verification (NuDiVe) 2022 exercise likewise featured the use of portal monitoring.

B. FUNCTIONAL VERIFICATION ACTIVITIES: MONITORING CONTAINERS, TRUCKS, RAILCARS, AIRCRAFT

B.1. Monitoring and tracking warhead movements – loading/unloading on railcars, trucks and possibly aircraft and tracking shipments.

INF: Locational restrictions in Treaty Article VIII specify that missiles and launchers subject to the treaty must be located at deployment areas, at support facilities, or in transit. Transit shall be completed within 25 days (Treaty Article VIII.4). Notification must be provided regarding each transit no later than 48 hours after its completion, including such information as the number of missiles or launchers that were in transit, the points, dates, and times of departure and arrival, and the mode of transport (Treaty Article IX.5(f)(i-iii)). Notification must be provided also of the missile or launcher's location and time at that location every four days during transit (Treaty Article IX.5(f)(iv)).

START I: Locations where treaty limited items are permitted must be identified. This could include parking areas for transportation means. (See Article VI provisions that apply to rail launchers of ICBMs). Site diagrams and/or geographic coordinates must be provided for all the locations (See paragraphs 4 to 6 of Annex J to the MOU). Notification must be provided for movement between locations (See Article VIII and Section II of the Notification Protocol). There are restrictions on the location of support equipment (transportation means) (see Article IV). There is a limitation of transit time between locations. (see paragraph 12 of Article IV and paragraph 10 of Article VI).

New START: The Treaty's Article IV provides locational restrictions for deployed and non-deployed delivery vehicles, outlining the types of facilities that those Treaty-Limited Items can be located at. Per Article IV.4, the transit of non-deployed ICBMs and SLBMs, as well as non-deployed ICBM launchers cannot exceed 30 days. The NST Protocol's Part Four, Section III lists notifications of specific types of movements, including exits of solid-fueled missiles from production facilities and heavy bombers' visits to areas outside of national territories that last for longer than 24 hours. Moreover, Type Two inspections (outlined by the NST Protocol's Part Five, Section VII.8) can be used to verify empty launch canisters, providing a precedent for inspecting empty rail cars, trucks, and other transport means for nuclear warheads. Additionally, in the presence of numerous containers in transit, procedures for inspecting containers declared to be non-nuclear can be drawn from New START's reentry vehicle inspection procedures, outlined in NST Protocol's Annex on Inspection Activities, Part Six, Section II.

Other initiatives: Abovementioned technical solutions for portal monitoring may apply.

C. FUNCTIONAL VERIFICATION ACTIVITIES: ON-SITE VISIT/ CHALLENGES AT DECLARED FACILITIES

C.1. Challenge inspection of a warhead transport truck/railcar secure storage/parking area, including inspections of randomly selected trucks or railcars to gather data on their mileage and movements recorded and to confirm the absence of warheads.

INF: The Protocol on Inspection Section VII.7 grants inspectors the right to inspect the interior of all vehicles at the inspection site "whose dimensions are equal to or greater than the dimensions specified" for treaty items. Such vehicles may be inspected at any time during an inspection, and no such vehicle shall leave the site or building under inspection until inspected at the exit (Protocol on Inspection Section VII.12-13).

START I: Under Annex I to the Inspection Protocol, inspectors have the right to confirm the numbers, and, if applicable, types, variants or versions of items of inspection that are specified for the facility to be inspected and declared for the inspection site and to confirm the absence of any other item of inspection at the inspection site. This Annex also provides procedures for the inspection of covered objects, containers, launch canisters, vehicles, and structures located at that site.

New START: Per NST Protocol's Part Five, Section VII.8, Type Two inspections give the inspecting party the right to confirm that all launch canisters within the boundaries of an inspection site that were declared to be empty are, in fact, empty. This provides a precedent for confirming that all declared empty trucks and railcars are, in fact, empty. Possible facilities that can be designated for Type Two inspections include loading and storage facilities for ICBMs and SLBMs, as well as their repair facilities, and this precedent can similarly be applied to support transport facilities under the closed system.

C.2. Challenge inspection of a container storage site or storage facility confirming the absence of warheads.

INF: According to the protocol for baseline, close-out, and short-notice inspections, a container that is declared to contain a treaty item and that is not sufficiently large to contain more than one treaty item is inspected via external observation and measurement of dimensions only (Protocol on Inspection Section VII.8). So is a structure or container not sufficiently large to contain a treaty item (Protocol on Inspection Section VII.9). A container that is declared not to contain a treaty item but is sufficiently large to contain one is inspected by weighing or interior observation, unless it is a launch canister containing an item not subject to the treaty, in which case it is inspected via external visual observation, linear measurement, and radiation detection (Protocol on Inspection Section VII.8). A space that is declared not to contain a treaty item but is sufficiently large to contain such an item is not subject to inspection if it is shown not to be accessible by the smallest treaty item or if a visual inspection of the interior from the entrance shows it does not contain a treaty item (Protocol on Inspection Section VII.10). During inspections of former bases and facilities, the burden is on the inspected party to demonstrate that a shrouded object larger than the smallest treaty item is not a treaty item, through partial shroud removal, measuring, weighing, or other methods (Protocol on Inspection Section VII.14).

START I: Under Annex I to the Inspection Protocol, inspectors have the right to confirm the numbers, and, if applicable, types, variants or versions of items of inspection that are specified for the facility to be inspected and declared for the inspection site and to confirm the absence of any other item of inspection at the inspection site. This Annex also provides procedures for the inspection of covered objects, containers, launch canisters, vehicles, and structures located at that site.

New START: Part Nine of the Annex on Inspection Activities outlines specific procedures for inspecting objects, covered objects, containers, vehicles, and structures. At each kind of base eligible for inspection, this part provides specific measurements that a given structure or object would need to exceed in order to be capable of containing a TLI (Annex on Inspection Activities, Part Nine.3). The same approach could be adapted to determine which structures could potentially contain warhead containers, thereafter designating them as eligible for confirming the absence of warheads within.

D. FUNCTIONAL VERIFICATION ACTIVITIES: DISPLAYS AND CLOSE-OUTS

D.1. Close-out inspections.

CTR: US visits to former warhead sites in Ukraine, Belarus, and Russia established contracts with local construction companies to bulldoze or blow up former bunker facilities and cover the facilities with rock and then concrete.

INF: Close-out inspections are covered under paragraph 4 of Article XI of the Treaty. The Protocol on Inspection Section VII.7 allows inspectors to "inspect the entire inspection site, including the interior of structures, containers or vehicles, or including covered objects, whose dimensions are equal to or greater than the dimensions specified." Support structures are eliminated in situ (Treaty Article X.4), and support equipment is removed, subject to verification by inspections.

START I: Close-out inspection procedures are covered under paragraph 9 of Article XI and Section XII of the Inspection Protocol. These procedures may be relevant in determining whether a warhead storage facility, rail/road transfer point, or other associated sites have been closed out and therefore warheads are no longer permitted to be present there. Formerly declared facility inspection procedures are covered under paragraph 10 of Article XI and Section XIII of the Inspection Protocol and may be relevant in determining whether any warhead-related activity is being conducted there.

New START: While the New START Treaty does not provide a category of close-out inspections specifically, the Treaty's Article XI.3 and the NST Protocol's Part Five, Section VII outline procedures for Type Two inspections of formerly declared facilities to verify that they are not being used for "purposes inconsistent with the Treaty." That includes inspecting facilities that have been converted to no longer house nuclear weapons and verifying the absence of those weapons by inspecting those facilities and individual delivery systems within them via a sampling approach, detailed in NST Protocol: Annex on Inspection Activities, Part Seven.

Other initiatives and precedents: Several international research initiatives (including IPNDV and UNIDIR-led efforts) have studied the applicability of gamma and neutron imaging techniques, as well as other on-site inspection procedures to the process for verifying the absence of nuclear warheads and material at a given facility. For instance, these initiatives also outlined use cases for tamper-evident seals, cameras, and cryptographic algorithms for authenticating the collected data and software of the devices used. Cryptographic authentication was also employed during implementation of the Open Skies Treaty.

D.2. Open display of warhead or container – performed in association with a transfer of custody at the beginning or end of a transportation shipment or performed randomly at negotiated times and frequency at or near a storage facility. This would be used to confirm declarations/notifications. The displays would be another entry into the warhead passports and could be correlated later through a data challenge.

INF: Continuous portal monitoring procedures provide for the opening of containers without removal of the item from the container to ensure that the item is, as declared, not an item subject to the treaty. In addition, cooperative measures provide for the removal of concealment and display of missiles and launchers in the open at the inspecting party's request to allow for verification via national technical means (Treaty Article XII).

START I: Displays in the open may be necessary to substitute for on-site inspections under certain circumstances, such as demonstrating that a warhead container, truck or railcar was empty. (See Article XII).

New START: In case of the ICBM, SLBM, and heavy bomber elimination, the NST Protocol's Part Three, Section II.3 allows for the use of National Technical Means to observe the eliminated missiles, bombers, and launch canisters for 60-day periods following the notification of its elimination. With these items required to be "visible to the national technical means of verification" for the entirety of the aforementioned period, the Treaty sets the precedent for similar language in relation to open displays of warhead containers.

D.3. Technical characteristics exhibition – exhibition of warheads/warhead containers, trucks, and railcars to facilitate confirmation of declarations/notifications, for example, at truck or railcar storage facilities by pulling out randomly selected railcar trays to show there are no warheads in the stored areas. This could be similar to open displays, but focused on the handling and transport systems for nuclear warheads.

INF: Data exchanges involved an initial declaration of the technical characteristics (including length, maximum diameter, height, and weight) of treaty items including missiles, launchers, support structures, and support equipment. The information was verified by one American and one Soviet team conducting independent measurements of the items in question at elimination sites. The measurements were taken as the standard for all subsequent inspections. In addition, the INF Treaty provided for the examination of inspection equipment and supplies by the in-country escort in the presence of the inspection team (Protocol on Inspection Section V.4).

START I: Technical characteristic exhibitions may be necessary to confirm the size and configuration of warheads and transportation means that may be observed during inspections or in displays in the open. (See paragraph 11 of Article XI and Section XIV of the Inspection Protocol.)

New START: Article XI.4 of the Treaty obliges both Parties to conduct exhibitions to the other party in order to demonstrate features and technical characteristics of new types of TLIs, as well as to demonstrate the results of conversation of the first item of each TLI type. Annex on Inspection Activities, Part Eight.3 lays out further details for exhibition procedures, enabling the inspecting party to make measurements of the exhibited items and record distinguishing features and technical data related to the item in accordance with regular inspection procedures. This approach could be similarly employed to conduct exhibitions for new types of warheads, containers, trucks, and railcars introduced into the closed system's monitoring regime.

E. FUNCTIONAL VERIFICATION ACTIVITIES: SUSPECT SITE INSPECTIONS

E.1. Suspect site challenge inspection at declared conventional warhead storage site, at a site not declared to contain either conventional or nuclear warheads.

INF: The treaty does not provide for inspections at undeclared or suspect sites, although the procedure for short-notice inspections, particularly inspections of former missile operating bases and support facilities, may offer reference.

START I: Suspect site inspections are covered under paragraph 5 of Article XI; the specific sites to be subject to such inspections would be agreed by the parties in advance.

New START: The treaty does not specify suspect-site inspections, but procedures for Type Two inspections at formerly declared facilities may offer relevant techniques and technologies for this function. Specifically, FDFs are declared to no longer have the capability for storing nuclear weapons, e.g. on heavy bombers, and the NST Protocol's Part Five and Annex on Inspection Activities, Part Seven outline the procedures that can be transferred to suspect-site inspections.

UK-Norway Initiative: Initiative participants explored managed access techniques including identity checks, searches, shrouding, exclusion zones, walkways, limits on time and the number of inspectors, escorting and monitoring, among others, to avoid interfering with facility operations and protect sensitive objects and information. While the scenario of the exercise is the verification of warhead dismantlement, the managed access procedures developed by the initiative are applicable to any challenge inspection, particularly at suspect sites, where the inspected party is likely to have concerns related to the protection of sensitive information.

Joint US-UK Verification: Like the UK-Norway Initiative, Joint US-UK Verification sought to develop and demonstrate verification technologies and managed access procedures that protect sensitive information while complying with the inspected facility's safety and security requirements.

Annex C. Draft Verification Protocol on Nuclear Warheads

DRAFT VERIFICATION PROTOCOL ON NUCLEAR WARHEADS

(NOTE: THROUGHOUT THIS TEXT, FOR EASE OF REFERENCE, DEFINED TERMS ARE IN ITALICS)

PREAMBLE

The United States of America and the Russian Federation, hereinafter referred to as the Parties,

In the interests of providing for the verification of a potential future agreement or agreements addressing *nuclear warheads,*

Have agreed as follows:

ARTICLE ONE

OBLIGATION TO PROVIDE DATA CONCERNING NUCLEAR WARHEADS

1. No later than __________ days after signature of this Protocol, each Party shall provide data on facilities and locations where *nuclear warheads* are or may be present on its territory or on the territory of a *basing country* or a *host country*. The data to be provided for each of the facilities and locations specified below shall include the site name and the number and type of *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars* present at that facility or location as of the date of signature of this Protocol:

(a) nuclear warhead storage facilities;
(b) nuclear warhead production/disassembly facilities;
(c) road-rail transfer points;
(d) rail transfer points;
(e) air transfer points;
(f) loading and unloading locations;
(g) nuclear warhead transport vehicle secure storage/parking areas;
(h) nuclear warhead transport railcar secure storage/parking areas;
(i) nuclear warhead air transport secure parking areas; and
(j) nuclear warhead container storage locations.

2. In addition to the above-mentioned obligation to provide the number and type of *nuclear warheads* for each facility or location, each Party shall provide, as a unique identifier, a non-repeating alpha-numeric number for each of its *nuclear warheads* that shall be used

in reference to that nuclear warhead for all purposes under this Protocol. That number shall be in the form of a *cryptographically generated unique identifier,* which may be derived from either:

(a) a physical tag or seal applied directly to the warhead or, if the warhead is never separated from its container during its service life, its container, as described in Annex 2 to this Protocol; or

(b) the *passport* of that warhead.

Cryptographically generated unique identifiers shall be created in accordance with the provisions of Article 2 and Annex 3 to this Protocol.

3. The Parties shall provide site diagrams of all facilities and locations specified in paragraph 1 of this Article. Each site diagram shall be identified by geographic coordinates, using the system of coordinates commonly employed by that Party, and shall include boundaries that, at a minimum, enclose the structures used for, and the area associated with, *nuclear warheads* and *nuclear warhead containers,* as well as the structures used to contain *nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, and nuclear warhead transport railcars.* The network of major roads within the boundaries shall be shown on the site diagram, but if the facility or location consists of two or more non-contiguous areas, the network of major roads connecting these separate areas shall also be shown.

4. Except for site diagrams of *nuclear warhead production/disassembly facilities,* and except for structures the entrances of which are not large enough to permit passage of *nuclear warheads,* all structures that are intended for, and are large enough to be used for, *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* or *nuclear warhead transport railcars* shall be depicted on the site diagram. Site diagrams for *rail transfer points* shall show all railway tracks, rail entrances/exits, and parking sites within that facility, as well as structures that are large enough to contain *nuclear warheads.* Site diagrams for *nuclear warhead storage facilities* shall identify all exit/entry points, including the main entry point/access point for the facility, the emergency exit point, and the access point at each of the bunkers.

5. Each Party shall provide a description of all routes used to transport *nuclear warheads,* including road, rail, and air routes. Where applicable, the routes shall indicate the network of major roads and railway tracks. The routes may be identified on a map and/or identified by their beginning and end points defined by their geolocation data. Each Party shall declare the number/range of hours required for transit on these routes between each of the facilities and locations specified in paragraph 1 of this Article.

6. The Parties shall notify each other of all changes in the data provided pursuant to this Article. No later than __________ days after the date of the change, the Parties shall provide updated data for each category of data in which the data has changed. In addition, the movement of *nuclear warheads* shall be notified separately, in accordance with Article Three of this Protocol.

7. The Parties shall use the U.S. National and Nuclear Risk Reduction Center (NNRRC) and its Russian counterpart to provide and receive the data and notifications specified in this Protocol and, for site diagrams, their diplomatic channels.

8. *Nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars* shall not be located anywhere other than the facilities or locations identified in paragraph 1 of this Article or shall be in *transit* between such facilities or locations. Transit shall be conducted along the routes specified in paragraph 5 of this Article and shall not exceed the number/range of hours declared, in accordance with paragraph 5, for transit between specific locations. On an exceptional basis, *nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars* may be moved for maintenance or repair to a facility or location other than those listed in paragraph 1 of this Article. Notification of such movement shall be provided at least __________ days before its departure and a separate notification shall be provided no more than __________ days after its return.

ARTICLE TWO

OBLIGATION TO MAINTAIN AND PROVIDE DATA FROM WARHEAD INVENTORY MANAGEMENT SYSTEM

1. In addition to the data provided for in Article One of this Protocol, each Party shall maintain logistical data on each of its *nuclear warheads,* from the time the warhead leaves a *nuclear warhead production/disassembly facility* until it arrives at a *deployment base,* or until its return to a *nuclear warhead production/disassembly facility,* in an *inventory management system*. Each Party shall have the right to use its own methodology to create its *inventory management system.*

2. Based on the data contained in their respective *inventory management systems,* the Parties shall create *passports* for each of its nuclear warheads of the following types:

(a) For the United States of America: ______________
(b) For the Russian Federation: ______________

The data fields to be included in each *passport* are set forth in Annex 3 to this Protocol.

4. The Parties shall share the *passport* of each of its *nuclear warheads,* accurate as of the date of signature of this Protocol, in the form of a *cryptographically generated unique identifier,* within __________ days of signature of this Protocol. Unless the Parties have agreed to use the same methodology to cryptographically generate unique identifiers, each Party shall have the right to use its own methodology for that purpose. Regardless of the methodology used, each Party shall provide, in response to a data challenge by the other Party, the cryptographic key to confirm the data that was used to produce the *cryptographically generated unique identifier.*

5. The Parties shall notify each other of any change in the *passports* of their *nuclear warheads*, no later than __________ days after the date of the change, in the form of updated *cryptographically generated unique identifiers* for the respective *nuclear warheads.*

6. The Parties shall use the U.S. National and Nuclear Risk Reduction Center (NNRRC) and its Russian counterpart to provide and receive their *cryptographically generated unique identifiers.*

ARTICLE THREE

OBLIGATION TO PROVIDE NOTIFICATION OF NUCLEAR WARHEAD MOVEMENTS

1. The movement of each *nuclear warhead* to another facility or location specified in paragraph 1 of Article One of this Protocol shall be added to the warhead's *passport* and shall be subject to a notification. The movement of *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars* to another facility or location shall be notified in accordance with paragraphs 6, 7 and 8 of Article One of this Protocol.

2. Provisions governing notification of *nuclear warhead* movements are contained in Annex 4 to this Protocol.

ARTICLE FOUR

DATA CHALLENGES

1. In order to increase confidence in the reliability of the data provided in the *cryptographically generated unique identifiers,* each Party shall have the right to initiate data challenges to the other Party that require that Party to reveal specified data contained within those *cryptographically generated unique identifiers.* The number of data challenges shall __________. The amount of data to be revealed in each data challenge, the timelines for responding to data challenges, and the methodology used to determine how the amount of data revealed in a data challenge applies to the quantitative limits on data challenges, shall be agreed between the Parties.

2. The procedures governing data challenges are set forth in Annex 5 to this Protocol.

ARTICLE FIVE

RIGHTS AND OBLIGATIONS WITH RESPECT TO THE USE OF THE zk-SNARK TOOL

1. The Parties have the right to request, and the obligation to cooperate in, the use of the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) tool with respect to specified *cryptographically generated unique identifiers.* The zk-SNARK tool shall be used to assess the integrity of the *passport* data without revealing the data. If the Parties agree that sensor data shall be encrypted, the zk-SNARK tool may be used to assess the integrity of that data and the consistency of that data corresponding to relevant *passport* data.

2. The procedures governing the use of the zk-SNARK tool are set forth in Annex 6 to this Protocol.

ARTICLE SIX

RIGHTS AND OBLIGATIONS WITH RESPECT TO ON-SITE INSPECTIONS

1. Each Party shall have the right to conduct, and the obligation to receive and facilitate, on-site inspections at facilities and locations specified in paragraph 2 of this Article. The number of on-site inspections shall __________. As provided for in paragraph 1 of Article Ten of this Protocol, a sensor data check may take place at the same time and at the same facility or location as an on-site challenge inspection. In such a case, the two activities shall count towards their respective quotas for that period, even if they are conducted by the same team.

2. On-site inspections may be conducted at the following facilities and locations, for the purposes indicated:

(a) at a *nuclear warhead storage facility:* to confirm the presence of a *nuclear warhead;* to confirm *declared data,* or to confirm the absence of any *nuclear warheads* at that facility;

(b) at a *rail transfer point,* an *air transfer point,* a *road-rail transfer point,* or a loading and unloading location: to confirm the presence of a *nuclear warhead* in vehicles, aircraft or railcars designated by the inspection team; to confirm *declared data;* or to confirm the absence of any *nuclear warheads* at that facility or location;

(c) at the designated entry/exit points to a *nuclear warhead production/disassembly facility:* to confirm the presence or absence of a *nuclear warhead* at that location or to confirm *declared data;*

(d) at a *nuclear warhead transport vehicle secure storage/parking area,* to confirm the presence or absence of *nuclear warheads* in a vehicle or vehicles designated by the inspection team;

(e) at a *nuclear warhead transport railcar secure storage/parking area,* to confirm the presence or absence of *nuclear warheads* in a railcar or railcars designated by the inspection team;

(f) at a *nuclear warhead air transport secure parking area,* to confirm the presence or absence of *nuclear warheads* in aircraft designated by the inspection team;

(g) at a *nuclear warhead container storage site,* to confirm the presence or absence of *nuclear warheads* in a container or containers designated by the inspection team; and

(h) at any other facility or location declared pursuant to paragraph 1 of Article One of this Protocol on the territory of the other Party or on the territory of a *basing country* or *host country,* to confirm the presence or absence of *nuclear warheads* in a container, vehicle, railcar, or structure designated by the inspection team.

3. On-site inspections may not be conducted during warhead transfer operations. The facilities and locations at which warhead transfer operations are being conducted shall be identified to the inspection team at its arrival at the point of entry, prior to the designation of the facility or location at which the inspection is to take place.

4. Each Party shall treat with due respect members of inspection teams, as well as members of sensor emplacement/removal observation teams and members of sensor data check teams, of the other Party present on its territory or on the territory of a *basing country* or *host country* in connection with verification activities under this Protocol, and shall take all appropriate measures, consistent with its national law, to prevent any attack on the person, freedom, and dignity of such personnel.

5. Members of inspection teams, as well as members of sensor emplacement/removal observation teams and members of sensor data check teams, shall take no actions affecting the safe operation of a facility, and they shall observe safety regulations established at the site.

6. The procedures governing the conduct of on-site inspections are forth in Annex 7 to this Protocol.

ARTICLE SEVEN

RIGHTS AND OBLIGATIONS WITH RESPECT TO CLOSE-OUT INSPECTIONS

1. Each Party shall have the right to close a facility or location specified in paragraph 1 of Article One of this Protocol if it is no longer being used for activities related to the storage, handling, or transport of *nuclear warheads* or if it is to be eliminated completely. Each Party shall have the right to use such facility or location for activities related to the storage, handling, or transport of conventional warheads, as provided for in Annex 8 to this Protocol.

2. Upon completion of the close-out inspection, the facility or location shall no longer be subject to the obligations contained in this Protocol, including notifications and inspections, with the exception of suspect-site inspections, as provided for in Article Eight of this Protocol.

3. The purpose of the close-out inspection shall be to confirm the absence of *nuclear warheads, nuclear warhead containers,* and *nuclear warhead support equipment and vehicles.* It shall also confirm notifications of the removal of the *nuclear warheads,* as well as to confirm any sensor data relating to the removal of the *nuclear warhead support equipment and vehicles.*

4. The procedures governing the conduct of close-out inspections are set forth in Annex 8 to this Protocol.

ARTICLE EIGHT

RIGHTS AND OBLIGATIONS WITH RESPECT TO SUSPECT-SITE INSPECTION

1. Each Party shall have the right to conduct suspect-site inspections at facilities and locations where *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles or nuclear warhead transport railcars* have not been declared or notified but regarding which a Party has concerns about the possible presence of such items. The facilities and locations subject to suspect-site inspections are specified in Annex 9 to this Protocol.

2. Following each suspect-site inspection conducted by the inspecting Party, the number of on-site inspections to which the inspecting Party is entitled, pursuant to Article Six of this Protocol, shall be __________.

3. The purpose of a suspect-site inspection is to confirm the absence of *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead security equipment, nuclear warhead transport vehicles* and *nuclear warhead transport railcars.*

4. The procedures governing the conduct of suspect-site inspections are set forth in Annex 9 to this Protocol.

ARTICLE NINE

OBLIGATIONS WITH RESPECT TO THE EMPLACEMENT, OPERATION, AND MAINTENANCE OF SENSORS

1. Each Party shall have the obligation to emplace, operate and maintain sensors at the facilities and locations specified in paragraph 1 of Article One of this Protocol, on routes described in paragraph 5 of Article One, and on *nuclear warhead support equipment and vehicles, nuclear warhead security equipment, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars.*

2. The types of sensors to be used to monitor the movement of *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead security equipment, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* are listed in Annex 10 to this Protocol.

3. The purpose of such sensors is to supplement or corroborate data that is provided in notifications on the movement of nuclear warheads or in other *declared data,* as well as in notification of changes in the location of *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars.* The sensors are also intended to detect the movement of undeclared *nuclear warheads* and the movement of any of the items specified in this paragraph outside declared areas.

4. The procedures governing the emplacement of sensors are set forth in Annex 10 to this Protocol, and the procedures governing the operation and maintenance of sensors are set forth in Annex 11.

ARTICLE TEN

RIGHTS AND OBLIGATIONS WITH RESPECT TO ON-SITE SENSOR DATA CHECKS

1. Each Party shall have the right to access data on-site from the sensors emplaced on the territory of the other Party, or on the territory of a *basing country or host country.* Such on-site sensor data checks shall __________. A sensor data check may take place at the same time and at the same facility or location as an on-site inspection.

2. On-site sensor data checks may be conducted at the following locations for the purposes indicated:

(a) *nuclear warhead transport vehicle secure storage/parking area,* including vehicles designated by the sensor data check team, to gather data on their recorded mileage, movements, opening and closing of doors and gates, and, as applicable, changes in weight and radiological measurements from sensors emplaced on entrances, exits, and doors;

(b) *nuclear warhead transport railcar secure storage/parking area,* including railcars designated by the sensor data check team, to gather data on their recorded mileage, movements, opening and closing of doors and gates, and, as applicable, changes in weight and radiological measurements from sensors emplaced on entrances, exits, and doors;

(c) *nuclear warhead container storage site or nuclear warhead storage facility,* to gather data from nuclear security sensors emplaced on entrances, exits, and doors; and

(d) any other location where sensors have been emplaced, to gather data from the sensors.

3. The procedures governing the conduct of on-site sensor data checks are set forth in Annex 12 to this Protocol.

ARTICLE ELEVEN

OBLIGATIONS OF THE PARTIES WITH RESPECT TO NUCLEAR WARHEADS AND FACILITIES LOCATED OUTSIDE OF THEIR NATIONAL TERRITORIES.

1. Each Party takes note of the assurances received from the other Party regarding understandings reached between the other Party and the *basing countries* and *host countries* to the effect that the *basing countries* and *host countries* have agreed to the conduct of inspections, the emplacement, operation and maintenance of sensors, and on-site sensor data checks, in accordance with the provisions of this Protocol, on their territories.

2. Each Party shall remain fully responsible towards the other Party for the implementation of its obligations under this Protocol in respect of the facilities and locations specified in paragraph 1 of Article One that are located on the territories of *basing countries* and *host countries,* as well as its *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* located there.

ARTICLE TWELVE

RIGHTS AND OBLIGATIONS WITH RESPECT TO DISPLAYS IN THE OPEN

1. Each Party shall have the right to make a request to the other Party for a display in the open of specified items and specified facilities and locations. The number of displays in the open shall __________.

2. A request for a display in the open may be made:

(a) in connection with a transfer of custody at the beginning or end of the transportation of *nuclear warheads,* for which, as applicable, the *nuclear warhead container, the nuclear warhead transport vehicle,* and the *nuclear warhead transport railcar* shall be opened, and the transport trays of the railcar pulled out;

(b) at or near a *nuclear warhead storage facility, nuclear warhead container storage area, nuclear warhead transport vehicle secure storage/parking area, nuclear warhead transport railcar secure storage/parking area,* or *nuclear warhead air transport secure parking area.*

3. The purpose of the display in the open shall be to facilitate the confirmation of *declared data.* Displays in the open may also be used in connection with close-out inspections of facilities and locations, pursuant to Article Seven of this Protocol.

4. The procedures governing requests for displays in the open are set forth in Annex 13 to this Protocol.

ARTICLE THIRTEEN

OBLIGATIONS WITH RESPECT TO TECHNICAL CHARACTERISTICS EXHIBITIONS

1. Each Party shall have the obligation to conduct a technical characteristics exhibition of each type of its *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, nuclear security equipment,* and *nuclear warhead transport railcars.* Such exhibitions shall be conducted in the presence of representatives of the other Party or conducted in another manner that is acceptable to the other Party. The Parties shall conduct the exhibitions within __________ days of the signature of this Protocol. The site of the technical characteristics exhibitions shall be chosen by the Party conducting the exhibition.

2. The purpose of technical characteristics exhibitions is to facilitate confirmation of *declared data.*

3. The procedures governing the conduct of technical characteristics exhibitions are set forth in Annex 14 to this Protocol.

ARTICLE FOURTEEN

USE OF NATIONAL TECHNICAL MEANS OF VERIFICATION

1. For the purpose of ensuring verification of compliance with the provisions of this Protocol, each Party shall use national technical means of verification at its disposal in a manner consistent with generally recognized principles of international law.

2. Each Party undertakes not to interfere with the national technical means of verification of the other Party operating in accordance with paragraph 1 of this Article.

ARTICLE FIFTEEN

ESTABLISHMENT OF A BILATERAL VERIFICATION COMMISSION

To promote the objectives and implementation of the provisions of this Protocol, the Parties hereby establish a Bilateral Verification Commission. The Parties agree that, if either Party so requests, they shall meet within the framework of the Bilateral Verification Commission to:

(a) resolve questions relating to compliance with the obligations assumed; and

(b) agree upon such additional measures as may be necessary to improve the viability and effectiveness of this Protocol.

ANNEX 1: TERMS AND THEIR DEFINITIONS

For the purposes of the Protocol:

1. The term "air transfer point" means any place where a *nuclear warhead* may be loaded on or unloaded from an aircraft, including planes, helicopters, or any other air conveyance.

2. The term "basing country" means any NATO country or Russian allied country on the territory of which *nuclear warheads* are or may be located.

3. The term "buddy tag" means a unique tag that travels with, but is physically removed from, a specific *nuclear warhead* and that serves as an identifier of that warhead for the inspection team.

4. The term "cryptographically generated unique identifier" means the unique digital identifier of a *nuclear warhead,* based on the data contained in its passport that is created using cryptographic techniques that use Merkle trees to generate *one-way hash codes* for each *nuclear warhead.*

5. The term "declared data" means:

(a) data with respect to *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars* that have been provided in accordance with Articles One and Three of the Protocol;

(b) data that has been revealed in accordance with the provisions of Article Four of the Protocol;

(c) Information on technical characteristics of *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles,* and *nuclear warhead transport railcars* that have been confirmed during technical characteristics exhibitions;

(d) Information that the inspected Party provides to inspection teams during pre-inspection procedures; and

(e) Any other information that has been exchanged between the Parties pursuant to the Protocol, including information on *nuclear security equipment.*

6. The term "deployment base" means an area in which one or more launchers of nuclear-armed or nuclear-capable ballistic or cruise missiles are located, or an airbase where one or more aircraft equipped to carry nuclear armaments are located.

7. The term "host country" means any NATO country or Russian allied country on the territory of which there are facilities or locations that are subject to inspection or sensor data checks under the provisions of the Protocol.

8. The term "inventory management system" means a system created by a Party that tracks *nuclear warheads* by locations, movements, and other transactions, such as DIAMONDS (Defense Integration and Management of Nuclear Data Services) and AICMS (Automated Inventory Management and Control System).

9. The term "King Tut block" means a large concrete structure with heavy rebar implanted that is difficult to remove without very heavy lifting equipment and is difficult to blow apart with explosives due to the high density of rebar installed within.

10. The term "limited lifetime component 1", as used as a data field in the *passport* of the *nuclear warhead,* means items agreed by the Parties for inclusion in a *passport* data field such as tritium components, neutron generators, and power-source batteries.

11. The term "limited lifetime component 2", as used as a data field in the *passport* of the *nuclear warhead,* means items agreed by the Parties for inclusion in a *passport* data field such as tritium components, neutron generators, and power-source batteries.

12. The term "loading and unloading location" means a location outside of a *deployment base* where *nuclear warheads* are loaded on or unloaded from any vehicle, railcar, aircraft, or any other conveyance.

13. The term "nuclear security equipment" means the physical security equipment used to protect *nuclear warheads* during permanent or temporary storage, and includes all fencing, gates, and sensors used to provide security measures.

14. The term "nuclear warhead" means any device designed to produce an instantaneous release of an amount of nuclear energy from special nuclear material that is greater than the amount of energy that would be released from the detonation of one pound of trinitrotoluene (TNT).

15. The term "nuclear warhead air transport secure parking area" means the area where aircraft used to transport *nuclear warheads* may be parked permanently or temporarily.

16. The term "nuclear warhead container" means a container directly associated with a *nuclear warhead* that can be or has been used for transporting and storing one or more *nuclear warheads.*

17. The term "nuclear warhead container storage site" means any building or room in which containers used to house *nuclear warheads* are stored.

18. The term “nuclear warhead production/disassembly facility” means a declared facility where *nuclear warheads* are assembled or disassembled and exchanged with the military forces of that Party.

19. The term “nuclear warhead storage facility” means a specified facility, outside of a deployment base, for the storage of *nuclear warheads.*

20. The term “nuclear warhead support equipment and vehicles” means *nuclear warhead* lifting and handling equipment, and *nuclear warhead* transportation and moving equipment and vehicles.

21. The term “nuclear warhead transport railcar” means a railcar that is used to transport *nuclear warheads* and nuclear security forces that accompany such railcars.

22. The term “nuclear warhead transport railcar secure storage/parking area” means an area where such railcars may be stored or parked permanently or temporarily.

23. The term “nuclear warhead transport vehicle” means any vehicle used to move nuclear warheads from one facility or location to another.

24. The term “nuclear warhead transport vehicle secure storage/parking area” means an area where such vehicles may be stored or parked permanently or temporarily.

25. The term “operation conducted” as used as a data field in the *passport* of the *nuclear warhead,* means any action that involved the physical on-site observation of a *nuclear warhead* (whether inside or outside of a container) or any action that involves touching, moving, or opening the container or warhead.

26. The term “one-way hash function” means an algorithm that derives a unique, inviolable digital fingerprint from any set of data that cannot be reversed to reveal the original data. The hash function shall also include the algorithmic key necessary to reveal the data represented by the hash code.

27. The term “passport,” with respect to *nuclear warheads,* means a unique data set of the operations and movements of a specified warhead used to identify and track *nuclear warheads* and their transactions.

28. The term “personnel,” as used as a data field in the *passport* of the *nuclear warhead,* means nuclear warhead escort personnel who have been given or allowed close proximity to a *nuclear warhead,* and whose identity is exchanged with the other Party.

29. The term “rail transfer point” means any location where a *nuclear warhead* may be loaded on or unloaded from a railcar.

30. The term “road-to-rail transfer” means any location where a *nuclear warhead* may be loaded on or unloaded from a vehicle to/from a railcar.

31. The term “secondary component, as used as a data field in the *passport* of the *nuclear warhead,* means a component of a *nuclear warhead* that is used to promote the critical detonation of nuclear material.

32. The term “status”, as used as a data field in the *passport* of the *nuclear warhead,* means a designator to distinguish active *nuclear warheads* in the stockpile from other warheads, such as warheads scheduled for dismantlement, warheads requiring maintenance or refurbishment (such as replacement of limited lifetime components), and reserve warheads. Each Party shall define the different designators it shall use in the “Status” field.

33. The term “transit” means the one-way movement from one facility or location to another facility or location, of a:

(a) nuclear warhead;
(b) nuclear warhead container;
(c) nuclear warhead transport railcar;
(d) nuclear warhead transport vehicle; or
(e) nuclear warhead support equipment or vehicle.

ANNEX 2: TAGS AND SEALS

1. Subject to agreement between the Parties, the Parties shall have the right to use tags to identify their *nuclear warheads.* The tag could be attached to a *nuclear warhead* or *nuclear warhead container* if it does not violate safety protocols, or the tag could be carried by designated in-country escorts, as *buddy tags,* and kept with its *nuclear warhead* wherever it may be.

2. Subject to agreement between the Parties, the Parties shall have the right to use other technologies to validate the identity of specific *nuclear warheads.*

3. Subject to agreement between the Parties, the Parties shall have the right to apply nonelectronic seals to any/all *nuclear warhead support equipment, nuclear security equipment, or equipment on nuclear warhead transport railcars* and *nuclear warhead transport vehicles.*

ANNEX 3: CRYPTOGRAPHICALLY GENERATED UNIQUE IDENTIFIERS

1. Each Party shall ensure that the passports used to create its *cryptographically generated unique identifiers* contain the following data for each *nuclear warhead*:

(a) Date/time group
(b) Location
(c) *Status*
(d) *Secondary component*
(e) *Limited lifetime component 1*
(f) *Limited lifetime component 2*
(g) *Operation conducted*
(h) *Personnel*
(i) Previous hash (if applicable)
(j) ID hash
(k) Explanation (if applicable, e.g., force majeure delay in transportation)

(l) Optional null field that can be used to insert another unique hash code that will be generated by the Party on a random basis representing random data selected by that Party.

2. This list of data fields may be amended by agreement of the Parties.

ANNEX 4: NOTIFICATION OF NUCLEAR WARHEAD MOVEMENTS

1. The Party conducting the movement of a *nuclear warhead* shall notify the other Party, no later than __________ days after the *nuclear warhead* has left its previously declared location, that the warhead was in transit to another location. Such notification shall include:

(a) its *cryptographically generated unique identifier* or the identification of its tag or seal;
(b) the date and time of its departure, as registered by a designated official of that Party;
(c) the name of the location from which the warhead departed;
(d) its mode of transport (rail, vehicle, air); and
(e) its intermediate and final destinations.

ANNEX 5: DATA CHALLENGE PROCEDURES

1. In accordance with Article Four of the Protocol, the challenging Party shall have the right to make data challenges relating to any data entry in a *passport* represented in a *cryptographically generated unique identifier.* Although data acquired from sensors is not included in the *passport* of a warhead and therefore are not subject to the provisions of this Annex, a Party shall have the right to challenge sensor data in accordance with the procedures provided for in Annex 11 to the Protocol.

2. A data challenge shall identify the data that it requests to be revealed by specifying one or more of the data fields specified in Annex 3 to the Protocol, as well as any other information that would permit the challenged Party to comply with the request.

3. The challenged Party shall reveal the requested data and shall demonstrate to the other Party how the data that it has revealed is consistent with the *cryptographically generated unique identifier.* The challenged Party shall provide to the other Party the same one-way hash function for that data that was used to produce the *cryptographically generated unique identifier* and the associated cryptographic key used to confirm the data. After the challenging Party processes the revealed data through that hash function, and the result is consistent with the *cryptographically generated unique identifier,* the revealed data shall be considered to be validated.

4. Data challenges may include, but are not limited to, the following:

(a) Identification of one or more *nuclear warheads* located at a specified location on a specified date or dates. The challenged Party shall reveal all the data recorded for that warhead or warheads, on that date/those dates at that location.

(b) Identification of any data provided for in paragraph 1 of Annex 3 for a specified *nuclear warhead* located at a specified location on a specified date. The challenged Party shall reveal the data for that warhead at that location on that date.

(c) Identification of the most recent location of a specified *nuclear warhead,* the date when a specified warhead became active, the most recent status of a specified warhead, and the date of the most recent transaction for a specified warhead. The challenged Party shall reveal the relevant data.

ANNEX 6: USE OF THE ZK-SNARK TOOL

1. For the purposes of using the zk-SNARK tool in the cryptographic data exchange methodology provided for in this Protocol, the validity of the data committed through the *passport* hash codes is determined by their adherence to the respective sets of predetermined rules that the *passports* must follow.

2. During the initial exchange of data provided for in Articles One and Two of the Protocol, each Party shall also provide a set of predetermined rules that apply to its *passports*. Subject to agreement between the Parties, each Party shall ensure that the predetermined rules cover the following categories:

(a) Data integrity, which shall include, but not be limited to, rules requiring that entries in the data fields for "Location," "Status," and "Operation Conducted" are based on data that has been provided pursuant to Article One of this Protocol, as well as rules governing which data fields cannot be empty;

(b) Chronological integrity, which shall include, but not be limited to, rules governing the sequence of *passport* entries in chronological order; and

(c) Operational logic, which shall include, but not be limited to, rules governing possible orderings of specified operations and durations of warhead movements for each declared route.

3. After the predetermined rules have been provided, the Parties shall designate a team of technical experts to develop the zk-SNARK tool. The tool shall incorporate the predetermined rules and cryptographic functions used by each Party in creating its *cryptographically generated unique identifiers.* Each Party shall have its own half of the zk-SNARK tool based on the cryptographic algorithms used to generate its *passport* hash codes.

4. When a Party provides notification of a change in the *passport* data in the form of an updated *cryptographically generated unique identifier,* in accordance with paragraph 5 of Article Two of the Protocol, or notification of *nuclear warhead* movements, in accordance with Article Three, the Party providing that notification shall also apply the zk-SNARK tool to the updated *passport* in order to generate proof of the validity of that update in accordance with the predetermined rule. That proof shall be included in the notification. The Party receiving the notification may use its half of the zk-SNARK tool to verify the proof provided by the other Party, by ensuring that the updated *cryptographically generated unique identifier* is valid according to the predetermined rules.

5. The zk-SNARK tool shall be designed to provide a proof of the validity of the updated *cryptographically generated unique identifier* if it meets all the predetermined rules or if the "Explanation" data field has a non-empty value. If an updated *cryptographically generated unique*

identifier does not meet the predetermined rules due to force majeure or another circumstance, the Party sending the notification shall include an entry in the "Explanation" data field.

ANNEX 7: ON-SITE INSPECTION PROCEDURES

1. The inspecting Party shall notify the inspected Party of its intent to conduct an on-site inspection no less than __________ days prior to the beginning of the inspection. The facility or location at which the inspection is to take place shall be designated to the inspected Party, in writing, no later than __________ after the arrival of the inspection team at the point of entry on the territory of the inspected Party or on the territory of a *basing country* or *host country.*

2. No later than __________ after the designation of the inspection site, the inspected Party shall implement pre-inspection restrictions at the inspection site, which shall remain in effect until the inspection team completes the pre-inspection procedures. During the period of time that pre-inspection restrictions are in effect, containers, support equipment, vehicles, and railcars large enough to contain a *nuclear warhead* of the inspected Party and covered objects large enough to contain or to be such items shall not be removed from the inspection site. The inspected Party shall close all gates and shall ensure that they remain so, by means of the emplacement of seals or tags on those gates, in accordance with procedures agreed between the Parties, until the arrival of the inspection team.

3. The inspected Party shall transport the inspection team from the point of entry to the inspection site no later than __________ after the time for the designation of the inspection site. Upon arrival at the inspection site, the inspection team shall have the right to designate a *nuclear warhead* for inspection by reference to its *cryptographically generated unique identifier,* its tag or seal, or by providing any other information that would permit the inspected Party to comply with the request. If the Parties have agreed to use *buddy tags* to accompany *nuclear warheads,* the inspection team shall have the right to inspect *buddy tags* at an agreed location at the facility, to confirm *declared data* relating to specific *nuclear warheads.*

4. In conducting an on-site inspection, the inspection team shall have the right, within the boundaries of the inspection site, to apply procedures of this Annex to covered objects, containers, vehicles, railcars, and structures that are large enough to contain or to be a *nuclear warhead,* in order to determine the presence or absence of a *nuclear warhead* therein. The inspection team shall be permitted to patrol the perimeter of the inspection site and station inspectors at the exits of the site for the duration of the inspection.

5. The inspection team shall also have the right to inspect *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* and their associated tags and seals that are present at that facility or location and to confirm that their presence has been notified in accordance with Article One or Article Three of the Protocol.

6. During the conduct of inspection procedures, inspectors shall use agreed size criteria to determine whether objects, covered objects, containers, trucks, railcars, and structures are large enough to contain *nuclear warheads.*

7. For an object that is located outside a container and is not covered, inspectors shall have the right to confirm whether such an object is a *nuclear warhead* by viewing, making measurements of its external dimensions at locations designated by a member of the in-country escort, and by using other technical measurements as agreed between the Parties.

8. The inspected Party shall have the right to take measures to protect sensitive installations and to prevent disclosure of confidential information not related to the purpose of the inspection. Such measures may include, inter alia, shrouding of sensitive displays, stores, and equipment.

9. For covered objects and containers, inspectors shall have the right to:

(a) If an object is covered or located in a container, view and make measurements of the dimensions of such a covered object or container to determine whether it is large enough to contain or to be a *nuclear warhead;*

(b) If a covered object or container is determined to be large enough to contain or to be a *nuclear warhead,* view and make dimensional measurements of such an object after the in-country escort has partially uncovered it or view and make measurements of the object within a container to determine whether such an object is a *nuclear warhead;* and

(c) If, upon completion of the procedures specified in subparagraphs (a) and (b) of this paragraph, inspectors are unable to determine whether the object is a *nuclear warhead,* view the object and make measurements of its external dimensions at locations designated by a member of the in-country escort after the in-country escort has fully uncovered the object or removed it from the container.

10. For objects that may be inside a vehicle or structure, inspectors shall have the right to:

(a) View and make measurements of the dimensions of any access to the vehicle or structure to determine whether such access is larger than the diameter, width, or height of a *nuclear warhead;*

(b) If such access is determined to be large enough to allow access, view and make measurements of the external dimensions of the vehicle or structure to determine whether such a vehicle or structure is large enough to contain a *nuclear warhead;*

(c) If the vehicle or structure is determined to be large enough to contain a *nuclear warhead,* inspect the interior of the vehicle or structure to determine the presence and the number of *nuclear warheads* in it.

(d) View and make measurements of the dimensions of any access to a partitioned or enclosed space within the vehicle or structure in accordance with subparagraph (a) of this paragraph and, if such access is determined to be large enough to allow access, inspect the interior of the partitioned or enclosed space to determine the presence and the number of *nuclear warheads* in it.

(e) Notwithstanding the right of the inspection team to inspect the interior of vehicles, structures, and partitioned and enclosed spaces within such vehicles or structures, pursuant to subparagraphs 10(c) and 10(d) above, if the inspected Party demonstrates to the satisfaction of the inspection team, by means of a visual inspection of the interior of a partitioned or enclosed space from its access, that the partitioned or enclosed space does not contain any object, such a partitioned or enclosed space shall not be subject to further inspection.

(f) For an object discovered inside a vehicle, structure, or partitioned or enclosed space within such a vehicle or structure, inspect it in accordance with paragraphs 13 and 14 of this Annex.

11. If, by viewing, measuring, and inspecting, the inspection team confirms that an object or covered object is not a *nuclear warhead,* or confirms that a container, vehicle, or structure does not contain a *nuclear warhead,* such an object, covered object, container, vehicle, or structure shall not be subject to further inspection, with the exception that the inspection team shall have the right to take linear measurements or have photographs taken to confirm that the item is a *nuclear warhead container, nuclear warhead support equipment or vehicle, nuclear warhead transport vehicle* or *nuclear warhead transport railcar.*

12. In conducting inspection activities, inspection teams shall have the right to use inspection equipment consisting of instruments and devices for making linear measurements, determining geographic coordinates, and taking photographs and videos, as specified in paragraph 13 of this Annex, for the purposes identified therein. The inspection teams shall also have the right to use the inspection equipment specified in paragraph 14 of this Annex, upon approval of the Parties, for the purposes identified therein. All inspection equipment shall be subject to examination each time it is brought into the country and shall be used in accordance with the procedures agreed between the Parties for each type of inspection equipment.

13. Inspection equipment approved for use by inspection teams during inspection activities:

(a) The inspection team shall have the right to use measuring tapes, range poles, and plumb bobs to determine length, width, and height of items to be inspected, as well as the dimensions of doors and openings in structures, vehicles, and railcars.

(b) Except for inspections at *nuclear warhead storage facilities,* the inspection team shall have the right to request through a member of the in-country escort that the inspected Party photograph, using a digital camera that shall include geo-location and date/time stamp data, an object, covered object, container, vehicle, railcar or structure located within the boundaries of the inspection site, for which questions or ambiguities remain between the inspection team leader and a member of the in-country escort or to confirm declared data on *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* and their associated tags and seals.

14. Inspection equipment subject to approval by the Parties for use by inspection teams during inspections activities:

(a) Hand-held thermal neutron detectors. The inspection team shall have the right to place hand-held thermal neutron detectors within 10 meters of a container, vehicle, railcar, or structure it has designated, to determine whether it contains more than the declared number of *nuclear warheads* as well as to confirm the presence or absence of *nuclear warheads.*

(b) Hand-held low resolution gamma ray detectors. The inspection team shall have the right to place hand-held low resolution gamma ray detectors within 10 meters of a container, vehicle, railcar, or structure it has designated, to determine whether it contains more than the declared number of nuclear warheads as well as to confirm the presence or absence of *nuclear warheads.*

(c) Hand-held ground penetrating radar devices. The inspection team shall have the right to use the devices at up to [5] locations within the designated site; and

(d) Portable mass weighing devices.

15. For the purposes of the Protocol, including during on-site inspections, the use of cameras shall be carried out in accordance with the following procedures:

(a) When photographs are taken by the inspected Party during an on-site inspection, the camera shall be visible at all times to the inspection team until the photographs are downloaded. The inspection team shall have the right to observe the downloading of the photographs. When the photograph is downloaded, a hash code that represents each photograph and the respective cryptographic key shall be produced and shared with the inspection team. The inspection team shall ascertain that the photographs are consistent with the associated hash code. The inspected Party shall transmit the hash code to the other Party through the NNRRC, with a physical copy given to the inspection team.

(b) When photographs are taken by a Party in conjunction with a transaction that results in an additional entry to the passport of its nuclear warhead, without the presence of the other Party, the photograph shall be downloaded and a hash code shall be produced, which shall be transmitted to the other Party through the NNRRC. A date/time stamp shall be included in the picture, which shall be made within [30] minutes after the transaction. The Party receiving the photograph may issue a data challenge of the associated passport data for the specified warhead in order to confirm the authenticity of the photograph, by determining whether the date/time stamp and picture are consistent with one another.

ANNEX 8: CLOSE-OUT INSPECTION PROCEDURES

1. The Party intending to close out a facility or location shall notify the other Party of its intent to close that facility or location. The notification shall include:

(a) the site name;
(b) its geographic coordinates;
(c) the planned date of the removal of the last *nuclear warhead, nuclear warhead container,* or *nuclear warhead support equipment or vehicles;*
(d) for n*uclear warhead storage facilities* that are to be totally eliminated, the planned date of the display in the open;

(e) whether, after the facility or location has been closed out, it is intended to be used for activities related to the storage, handling, or transport of conventional warheads; and
(f) the proposed date of the close-out inspection.

Any changes to the planned dates specified in subparagraphs 1(c) and 1(e) above shall be notified to the other Party no less than __________ prior to the date initially declared.

2. The removal of each *nuclear warhead* from the facility or location shall be subject to a notification in accordance with Article Three of the Protocol. The *passport* for each of the *nuclear warheads* that had been present at the facility or location shall include the date/time of the removal of the *nuclear warhead* from that facility or location. All *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* present at the facility or location shall be removed, notification of which shall be provided in accordance with paragraph 6 of Article One.

3. Except as provided for in paragraph 10 of this Annex, a Party intending to close out a facility or location shall remove or eliminate, all *nuclear warhead containers, nuclear warhead support equipment and vehicles,* environmental controls, and all storage and transport containers capable of containing a *nuclear warhead.* The removal or elimination of such items shall be confirmed, at the option of the other Party, by a close-out inspection or by national technical means of verification. For *nuclear warhead storage facilities* that are to be totally eliminated, the removal or elimination of such items shall take place only after the display in the open has been conducted and shall be confirmed by a close-out inspection.

4. For *nuclear warhead storage facilities* that are to be totally eliminated, the Party intending to close out such a facility shall also remove or eliminate:

(a) after the display in the open has been conducted, all cranes and handling equipment including forklifts and gurneys, with the exception of the crane used for placement of the *King Tut blocks* that shall be removed after the close-out inspection;

(b) all nuclear security equipment and devices within and around the *nuclear warhead* storage bunkers, including all containers;

(c) all equipment from the security control room; and.

(d) all sensors, including fence disturbance systems, microwaves, and cameras, but the fencing may be left in place around the bunkers and around the perimeter of the facility.

5. For *nuclear weapon storage facilities* that are to be totally eliminated, the Party intending to close out that facility shall take photographs of each of the empty bunkers after all equipment has been removed, and the photographs shall be provided to the inspection team at the time the inspection team arrives at that facility for the close-out inspection.

6. The display in the open at a nuclear warhead storage facility that is to be totally eliminated shall continue for a period of __________ days, during which all of its on-site handling equipment, including overhead cranes removed from the bunkers, forklifts, and gurneys, and the HVAC main system shall remain visible.

7. If the inspecting Party intends to conduct a close-out inspection, it shall notify the other Party of its agreement to the planned date of the inspection or provide an alternate date.

Once the Parties have agreed on the date for the close-out inspection, the inspecting Party shall notify the other Party, no less than __________ days in advance, of the estimated time of arrival of the inspection team at the point of entry of:

(a) the point of entry;
(b) the date and estimated time of arrival at the point of entry; and
(c) the names of the members of the inspection team.

The inspected Party shall transport the inspection team to the site specified in the notification provided in accordance with paragraph 1 of this Annex no later than __________ after its arrival at the point of entry. During the course of each close-out inspection, inspectors shall have the right to confirm that the close-out procedures provided for in this Annex have been completed.

8. For a close-out inspection of a *nuclear warhead storage facility* that is to be totally eliminated:

(a) the inspection team shall have full access to all parts of the warhead storage area, including within each of the storage bunkers, and shall have the right to view and take measurements pursuant to paragraph 9 of this Annex;

(b) The inspection team shall place seals on each door or gate of the fencing around each storage bunker after the inspection of that bunker has been completed, and, at the completion of the inspection of all the storage bunkers, the inspection team shall seal the perimeter of the warhead storage area with a fiber optic seal strung through the fencing of the entire perimeter at its upper and lower most heights, at locations designated by the inspection team;

(c) the inspected Party shall transport a *King Tut block* for each storage bunker at the site and, using a crane, shall place the block at the exit/entry point at each of the bunkers, at the direction and supervision of the inspection team. Depending on the configuration of the exit/entry point, the block shall be placed in front of a door or gate to preclude exit or entry. The inspection team shall place a seal on the *King Tut block* in front of each of the storage bunkers after the *King Tut block* has been emplaced. Upon completion of the close-out inspection, the crane shall be removed and shall be loaded onto a vehicle or railcar and transported away from the facility;

(d) the inspection team shall record the date/time on the seals as they are affixed at each location on the site and so that the inspecting Party is able to identify each of the unique seals during a future inspection.

9. For a close-out inspection of all facilities and locations, the inspection team shall have the right to:

(a) full access to the inspection site, which shall include:

(i) the right to view the interior of each structure or storage bunker to confirm the absence of items specified in paragraph 3 of this Annex, as well as cranes and handling equipment, including forklifts and gurneys; and

(ii) the right to make measurements of the dimensions of the structure or storage bunker or of the dimensions of the accesses into the structure or bunker and the dimensions of the partitioned or enclosed space within the structure or bunker or of the dimensions of the accesses into such a space; and the right to view the interior of the structure or bunker or the partitioned or enclosed space within the structure or bunker from a place designated by a member of the in-country escort. This place shall be designated in such a way as to allow the inspectors to view the entire interior of the structure or bunker or the partitioned or enclosed space within the structure or bunker.

(b) conduct its inspection within a period of __________ hours; and

(c) use the following verification equipment, in addition to those provided for in paragraphs 13 and 14 of Annex 7 to the Protocol:

(i) handheld ground penetrating radar system and other technologies to look for underground bunkers or adits on site that may not be visible;

(ii) radiological detectors to determine whether the object is non-nuclear;

(iii) if agreed to by the inspected Party, more intrusive measures such as the Fieldable Nuclear Material Identification System, cosmic ray muon imaging and/or portable fission meters.

10. For a facility or location that a Party intends to use for activities related to the storage, handling, or transport of conventional warheads, or for any other purpose not prohibited under the terms of the Protocol, that Party shall have the right to leave in place environmental controls. If *nuclear security equipment* is not removed or eliminated at such a facility or location, only those tags, seals and sensors affixed or attached to such equipment at the exterior gate shall remain in place, including any nuclear detector equipment located at the exit.

ANNEX 9: SUSPECT-SITE INSPECTION PROCEDURES

1. The inspecting Party shall notify the inspected Party of its intent to conduct a suspect-site inspection no less than __________ days prior to the beginning of the inspection. The facility or location at which the inspection is to take place shall be designated to the inspected Party, in writing, no later than __________ after the arrival of the inspection team at the point of entry on the territory of the inspected Party or on the territory of a *basing country* or *host country.*

2. No later than __________ after the designation of the inspection site, the inspected Party shall implement pre-inspection restrictions at the inspection site, which shall remain in effect until the inspection team completes the pre-inspection procedures. During the period of time that pre-inspection restrictions are in effect, containers, support equipment, vehicles, and railcars large enough to contain a *nuclear warhead* of the inspected Party and covered objects large enough to contain or to be such items shall not be removed from the inspection site. The inspected Party shall transport the inspection team from the point of entry to the inspection site no later than __________ after the time for the designation of the inspection site.

3. Each Party shall have the right to conduct suspect-site inspections at a facility or location on the territory of the other Party that meets any of the criteria set forth below:

(a) It has the characteristic signature of a *nuclear weapons storage facility,* which may include bunkers typical for each Party, the presence of typical transportation nodes for such a facility, overhead cranes, trolleys, tracks, nuclear-security systems, and other infrastructure such as temperature and humidity control systems, unless the other Party can demonstrate that it does not store *nuclear warheads.*

(b) It possesses containers large enough to contain a *nuclear warhead,* or possesses support equipment, vehicles, or railcars similar to those present at the facilities and locations specified in paragraph 1 of Article One of the Protocol, unless the other Party can demonstrate that these items are not being used to contain, support or transport *nuclear warheads.*

(c) It was subject to a close-out inspection in accordance with the provisions of Annex 8 to the Protocol but subsequently meets the criteria set forth in subparagraphs 3(a) and 3(b) above.

(d) After it was closed out in accordance with the provisions of Annex 8 to the Protocol, it is used for activities related to the storage, handling, or transport of conventional warheads.

(e) It is on a list of facilities and locations that the Parties agreed shall be subject to suspect-site inspections.

4. Each Party shall have the right to conduct suspect-site inspections at a facility or location on the territory of a *basing country* or *host country* if *nuclear warheads* had ever been present at that facility or location. The Parties shall agree on a list of such facilities and locations.

5. Each Party shall have the right to conduct no more than __________ suspect site inspection at any one time. Each Party shall have the right to conduct no more than __________ such inspections each year at the same facility.

6. The inspection team shall have the right to inspect the entire inspection site, in accordance with the procedures provided for in Annex 7 to the Protocol, unless the Parties agree otherwise. In this connection, the inspected Party shall have the right to take measures to protect sensitive installations and to prevent disclosure of confidential information not related to the purpose of the inspection. Such measures may include, inter alia, shrouding of sensitive displays, stores, and equipment.

7. In conducting a suspect-site inspection, inspection teams shall have the right to use the inspection equipment provided for in paragraphs 13 and 14 of Annex 7 to the Protocol, which shall be used in accordance with the procedures agreed between the Parties for each type of inspection equipment.

ANNEX 10: EMPLACEMENT AND REMOVAL OF SENSORS

1. The types of sensors to be emplaced on *nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles, nuclear warhead transport railcars,* and *nuclear warhead containers,* and at the facilities and locations specified in paragraph 1 of Article One of the Protocol, and along the routes used to transport *nuclear warheads* described in paragraph 5 of Article One, shall consist of the following:

(a) For *nuclear warhead transport vehicles* and *nuclear warhead transport railcars:*

(i) sensors that record the loading, the time, date, and the opening and closing of doors and that measure the presence or absence of an object in the vehicle or railcar that may include tie-down sensors, and/or weight measuring sensors;

(ii) navigational/route measuring devices that record the routes taken and locations over time using, for example, an inertial sensor; and

(iii) radiation detecting sensors, such as thermal neutron detectors and low resolution gamma ray spectroscopy systems, or particle track detectors and/or fission foils to detect and record when *nuclear warheads* were inside the vehicle or railcar.

(b) For *nuclear warhead support equipment and vehicles:*

(i) sensors to collect data on the locations and movements, including the date and time of the lift and transfer, of *nuclear warhead* handling equipment, such as forklifts used to remove a *nuclear warhead* from a vehicle and carry it to a railcar.

(c) For *nuclear warhead containers* that do not contain a *nuclear warhead:*

(i) sensors to identify when a seal was emplaced on the container and when it was broken in order to conduct a specified operation.

(d) For facilities, locations, along routes used to transport *nuclear warheads,* and for *nuclear security equipment:*

(i) sensors on doors, gates, and other entryways where *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* pass through, to record the time of opening and closing, as well as to identify the item passing through. For facilities and locations with emergency exits, seals may be affixed onto the emergency exits rather than sensors;

(ii) remote monitoring and surveillance cameras to take a video or photograph of each *nuclear warhead, nuclear warhead container, nuclear warhead support equipment and vehicle, nuclear warhead transport vehicle* and *nuclear warhead transport railcar* that passes through the doors, gates, or other entryways. Such cameras could be operated remotely, taken by remote controlled robots or robotically controlled devices, or operated by designated personnel at that facility or location;

(iii) cameras and weigh-in-motion sensors at key locations along transportation routes, to record the date and time when *nuclear warhead transport vehicles* and *nuclear warhead transport railcars* traverse those routes;

(iv) sensors at conventional warhead storage facilities to detect the presence of *nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles and nuclear warhead transport railcar;* and

(v) radiation detection sensors, such as thermal neutron detectors and cosmic ray muon imaging and fission signatures, at the entrances to warhead bunkers to detect the entry or exit of *nuclear warheads.*

2. Each Party shall have the right to observe the emplacement and removal of sensors by the other Party on items listed in paragraph 1 of this Annex, and at facilities or locations, or along routes used to transport *nuclear warheads,* on the territory of the other Party or on the territory of a *basing country* or *host country* of that Party. The Party emplacing or removing the sensors shall notify the other Party, no less than __________ days prior to the proposed date for the emplacement or removal of the sensors, of:

(a) the proposed date for the emplacement or removal of the sensors;

(b) the type of sensors to be emplaced or removed and the serial number of each such sensor;

(c) the items or objects on which the sensors are to be emplaced, or from which they are to be removed; and

(d) the location of the items or objects on which sensors are to be emplaced or from which they are to be removed.

For sensors that are to be removed or eliminated in connection with the removal or elimination of the item to which the sensor was emplaced, the Party removing or eliminating that item shall provide to the other Party a description of the elimination procedures for that item, including where that elimination is to take place, no less than __________ days prior to its elimination.

3. The Parties may agree, no later than __________ days after the notification provided in accordance with paragraph 2 of this Annex, that the emplacement or removal of such sensors may be carried out without on-site observation. In such case, the Party carrying out the emplacement or removal of the sensors shall provide, upon completion of the emplacement or removal of the sensors, video/picture confirmation of that activity, which shall include the serial numbers of those sensors.

4. If a Party intends to exercise its right to observe the emplacement or to observe the removal of sensors on the territory of the other Party or on the territory of a *basing country* or *host country,* it shall notify the other Party, no later than __________ after the notification provided in accordance with paragraph 2 of this Annex, of the date of the intended arrival of the sensor emplacement/removal observation team at the point of entry.

5. All sensors, tools, equipment, and supplies brought by the sensor emplacement/removal observation team shall be subject to examination by the in-country escort, in the presence of the team, upon its arrival at the point of entry. The purpose of such examination shall be to ascertain to the satisfaction of each Party that the sensors, tools, equipment, or supplies cannot perform functions unconnected with the verification activities of the Protocol.

6. The sensor emplacement/removal observation team shall provide to the in-country escort:

(a) installation drawings, installation manuals, and other documentation, including any changes made to such documentation, to be used to emplace or test the sensors; and

(b) manuals and any other documents, including any changes made to such documentation, to be used to operate and maintain the sensors.

If the Parties agree that, pursuant to paragraph 3 of this Annex, the emplacement of the sensors is to be carried out without on-site observation, such drawings, manuals, and other documents shall be provided through diplomatic channels, as well as the types and serial numbers of all the sensors to be emplaced.

7. The Parties shall ensure that all sensors to be emplaced are equipped with tamper-proof seals and designed so that they collect the data without transmitting it in real time. The sensors shall be emplaced or removed in the presence of the sensor emplacement/removal observation team, unless otherwise agreed by Parties in accordance with paragraph 3 of this Annex.

8. If requested, the Party emplacing or removing sensors on its territory or on the territory of a *basing country* or *host country* shall provide the following logistical support, at the expense of the other Party, for:

(a) all utilities for the emplacement or removal of the sensors;

(b) the site preparation for the emplacement of the sensors, which may include utility connections; and

(c) transportation of the sensor emplacement/removal observation team to the site, as well as all tools, equipment and supplies necessary for the emplacement or removal of the sensors.

9. Sensors for *nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* shall be emplaced or affixed when those items are not in use. This process shall be accomplished at secure parking areas or at nearby neutral, non-sensitive areas. The Parties shall agree upon the facility or location where the sensors would be affixed on newly produced *nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* and where the sensors would be removed upon disposal of any such items that reach the end of their service life. In all instances, the sensor emplacement/removal observation team shall not interfere with ongoing activities at the facility or location where the sensors are emplaced or removed, shall not hamper or delay operations at that facility, and shall take no actions affecting its safe operation. In carrying out its activities, the team shall observe safety regulations established at the facility including those for personal safety, as well as regulations for the protection of equipment and maintenance of the controlled environment within a facility.

ANNEX 11: OPERATION AND MAINTENANCE OF SENSORS

1. Each Party, in fulfilling its obligation to operate and maintain sensors on its territory and on the territory of a *basing country* or *host country,* shall notify the other Party of any issues related to their operation or maintenance that could affect data collected by the sensors. Such notification shall be provided no later than __________ days after the issue was identified, and shall include:

(a) the date the issue was identified;
(b) the serial number of the sensor;
(c) the item or object on which the sensor is emplaced;
(d) the location of the item or object on which the sensor is emplaced;

(e) a description of all maintenance, testing, or repair that has been carried out, or is intended to be carried out, and where that maintenance, testing or repair has or is to be carried out. The description shall include references to the drawings, manuals and documentation for such sensors provided pursuant to paragraph 6 of Annex 9 to the Protocol; and

(f) the date of completion, or planned date of completion, of the maintenance or repair.

2. If the Parties have agreed, pursuant to Annex 2 to the Protocol, to use seals on items to which sensors are attached, or on the sensors themselves, the notification shall include the date on which the seal was broken or is intended to be broken, the methodology used to break the seal, and, if the seal has been or is to be re-attached, the date of the completion or anticipated completion of that action.

3. If requested, the Party operating and maintaining sensors on its territory or on the territory of a *basing country* or *host country* shall provide the following logistical support, at the expense of the other Party, for:

(a) all utilities for the operation and maintenance of the sensors;
(b) site maintenance to ensure reliable operation of the sensors; and
(c) transportation of personnel to the site to operate, repair, test, or maintain the sensors, as well as all tools, equipment and supplies necessary for such activities.

ANNEX 12: ACQUISITION OF SENSOR DATA

1. In accordance with the provisions of this Annex, each Party shall have the right to acquire data collected by sensors that have been emplaced, pursuant to Annex 9 to the Protocol, on *nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles, nuclear warhead transport railcars,* and *nuclear warhead containers,* and at the facilities and locations specified in paragraph 1 of Article One of the Protocol, and along the routes used to transport *nuclear warheads* described in paragraph 5 of Article One.

2. A Party may acquire such data in any one of the following ways:

(a) by a sensor data check team, during an on-site sensor data check, as described in paragraphs 3, 5, 6, 7, 8, and 9 below;

(b) by an inspection team during an on-site inspection, as described in paragraphs 4, 5, 6, 7, 8, and 9 below; or

(c) by the Party on whose facilities and items the sensors have been emplaced, in response to a data challenge initiated by the other Party pursuant to Article Four of the Protocol, as described in paragraph 10 below.

3. The Party that intends to exercise its right to conduct an on-site sensor data check shall notify the other Party no less than __________ days prior to the beginning of the on-site sensor data check. The facility or location at which the on-site sensor data check is to take place shall be declared, in writing, no later than __________ after the arrival of the sensor data check team at the point of entry on the territory of that Party or on the territory of a

basing country or *host country.* The team shall be transported from the point of entry to the facility or location where the on-site sensor data check is to take place no later than __________ after the designation of that facility or location.

4. The Party that intends to exercise its right to conduct an on-site sensor data check during an on-site inspection shall so indicate to the inspected Party when the facility or location to be inspected is designated to the inspected Party, in accordance with paragraph 1 of Annex 7 to the Protocol.

5. Upon arrival of the team at the designated facility or location, the in-country escort shall provide the team with a simplified site diagram of the facility or location that indicates where all of the sensors are located, including sensors emplaced on *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles* and *nuclear warhead transport railcars* that are present at the facility at that time. If any of those items is absent at the time of the arrival of the team at the facility, the in-country escort shall inform the team of the reason for the absence of that item.

6. The team shall specify the nuclear warhead containers, *nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles* or *nuclear warhead transport railcars* on which the sensors to be checked have been emplaced. Until the team has completed the sensor data check for those sensors, none of the specified items shall leave the site.

7. The team shall have the right to bring and use equipment to conduct the on-site sensor data check after that equipment has been examined by the in-country escort, consistent with the procedures provided for in paragraph 5 of Annex 10 to the Protocol.

8. The team shall have the right to check the sensors in any order. The team shall carry out the sensor data check in the presence of the in-country escort and in accordance with the procedures contained in the manuals and other documents specified in paragraph 3 of Annex 10 to the Protocol. Data obtained from the sensors shall be certified by the signatures of a member of the team and a member of the in-country escort immediately after they are accessed.

9. The team shall not interfere with ongoing activities at the facility or location where the sensors are emplaced, shall not hamper or delay operations at that facility, and shall take no actions affecting its safe operation. In carrying out its activities, the team shall observe safety regulations established at the facility including those for personal safety, as well as regulations for the protection of equipment and maintenance of the controlled environment within a facility.

10. In order to respond to a sensor data challenge, the Party on whose facilities the sensors have been emplaced may need to acquire data relevant to that challenge by examining such sensors on-site or by remote retrieval of that data. In the former case, a notification shall be provided to the other Party that indicates the anticipated time required to respond to the challenge and any explanation if the anticipated time exceeds __________ days. Once the data is acquired, it shall be provided to the other Party by a notification or through diplomatic channels, in either unencrypted form or in a cryptographic hash code, as agreed between the

Parties. If the data is to be provided in a cryptographic hash code, the procedures set forth in paragraph 3 of Annex 5 to the Protocol shall be carried out in order to reveal that data. The timelines for responding to sensor data challenges shall be agreed between the Parties.

ANNEX 13: DISPLAYS IN THE OPEN

1. The notification of a request for a display in the open shall specify the facility or location where such a display is to take place and the items at that facility or location to be displayed. The display shall begin no later than __________ after the request is made and shall continue until __________ have elapsed from the time that the request was made. If such an open display cannot be conducted at that time, the requested Party shall respond no later than __________ after the request was made, provide an explanation for the delay and propose another date.

2. Annex 8 to the Protocol sets forth the obligations with respect to displays in the open for closing a facility or location.

ANNEX 14: TECHNICAL CHARACTERISTICS EXHIBITION

1. Each Party shall conduct, no later than __________ days after signature of the Protocol, technical characteristics exhibitions of each type of its *nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles* and *nuclear warhead transport railcars.* The purpose of such technical characteristics exhibitions is to facilitate verification of compliance with the provisions of the Protocol, as well as to determine where sensors may be emplaced on such items, if not already agreed between the Parties. The Parties may agree on additional items to be subject to technical characteristics exhibitions.

2. Such exhibitions shall be pre-scheduled by agreement between the Parties. The sites for such exhibitions shall be chosen by the Party conducting the exhibitions.

3. The team observing the exhibition shall arrive on the territory of the Party conducting the exhibition no later than one day and no earlier than three days before the scheduled exhibition date. The team shall be transported to the exhibition site so that it arrives at the site in a timely manner.

4. Prior to the commencement of the technical characteristics exhibition at the site, a member of the in-country escort shall:

(a) inform the team of the type of the items to be exhibited; and
(b) point out to the team, when applicable, in photographs, slides or drawings, the external differences that distinguish any of these items from similar items used for activities related to the storage, handling or transport of conventional warheads.

5. The Party conducting the exhibition shall provide the team with the opportunity to:

(a) view the item from a location designated by the in-country escort;
(b) make measurements, if applicable, at locations designated by a member of the in-

country escort in order to confirm the technical data for recognition of that item;

(c) View, confirm, and record each of the declared distinguishing features of such an item.

6. At the request of the team leader, a member of the in-country escort shall photograph each exhibited item in order to obtain __________ photographs of each such item. A member of the in-country escort shall provide one copy of each such photograph to the team leader prior to the completion of the exhibition.

Annex D. Preparatory Steps and Enhanced Verification Measures

This Annex describes a series of steps that could be taken prior to conclusion of a potential legally binding warhead agreement that sets maximum aggregate limits on nuclear warheads. It also presents an enhanced verification regime, based on and in part going beyond the measures set forth in the draft Verification Protocol (Annex C)[10] for such an agreement.

These enhanced verification measures include periodic inspections and additional data gathering and data assessment procedures that would be used to help validate periodic declarations by affixing sensors to storage, handling, transport, and security equipment. The goal is to develop an approach with multiple overlapping verification methodologies that could generate the confidence that would be required to pursue an agreement addressing total warhead stockpiles – and to do so without greatly increasing intrusiveness and thus increasing negotiability.

It is important to recognize that on 19 July 2024, the U.S. State Department unilaterally issued an updated declaration of the U.S. warhead inventory,[11] a measure that can be viewed as a potential preliminary step to encourage a potential future agreement addressing nuclear warheads. This paper and its Annexes provide additional potential bilateral steps that could be taken to address warhead inventories if and when Russia and possibly China were to express a willingness to open discussions on warheads.

A. PREPARATORY STEPS AND AGREEMENTS

The implementation of the verification protocol and the approach to developing a regime to address nuclear warheads, would require a number of preparatory steps prior to signature and EIF. Following the step-by-step approach recommended throughout this paper, some of those steps have been identified that could and should be pursued in order to build confidence and expertise required to support a warhead limitation agreement. These steps could be pursued sequentially or in parallel – depending on the willingness of Russia to join such efforts.

The preparatory steps would consist of a series of political commitments and/or government-to-government agreements and declarations that would serve as precursors to a potential agreement limiting nuclear warheads.[12] Throughout this Annex, we refer to

[10] The draft verification protocol (Annex C) is written as a stand-alone protocol that could be used for either a legally binding warhead agreement or a political commitment.

[11] https://www.state.gov/transparency-in-the-u-s-nuclear-weapons-stockpile-2/.

[12] A legally binding agreement that reduces or limits nuclear warheads cannot enter into force until after the U.S. Senate and the Federation Council of the Russian Federation have completed hearings and consented to its ratification, which can take a very long time. This means that the maximum warhead limits cannot take effect as a matter of law until entry into force (EIF) of that agreement. But most of the verification provisions could begin to apply prior to EIF: the Verification Protocol could be concluded as a separate government-to-government agreement - and then, once the warhead agreement enters into force, the Verification Protocol would be made an integral part of it. There is a precedent for this: the Ballistic Missile Launch Notification Agreement of May 31, 1988, was signed and implemented before START I signature and was incorporated into START I upon EIF.

elements of the draft verification protocol, for the preparatory government-to government/executive agreements and for the official baseline and initial verification steps that would be required under a final agreement.[13]

Each of the steps below would likely be pursued by working groups with different sets of experts such that some steps may be pursued in parallel rather than sequentially. Our notional approach proceeds logically beginning with the steps easiest to agree upon and most necessary to take subsequent steps. Most, if not all, of these working groups should conclude their work prior to signature of the treaty and/or the verification protocol, and indeed the results of these working groups should influence, and be incorporated in, the final texts of the treaty and the verification protocol.

Our suggested initial steps would not require the sides to agree to pursue a warhead limitation agreement and could have multiple applications for alternative arms control agreements. For example, elements of the Warhead Tracking System could be used to track other treaty limited items such as: the creation of unique identifiers; the development of computer systems;; and the development of passports. These steps should be carried out early on to ensure that the baseline data exchange can be conducted prior to the baseline verification measures.

STEP 1: *Technical Exchange to establish the process and to* ***create cryptographic unique identifiers*** *using both American and Russian cryptographic techniques combined into a joint software code to be used to produce the unique identifiers. Using notional sample data, the sides will test the process and jointly build the code, including conducting red team tests as necessary. If needed by either side, a government-to-government/executive agreement could be signed by both sides to establish this exchange.*

STEP 2: *Technical Exchange to jointly develop* ***dedicated computer hardware*** *systems to produce cryptographic unique identifiers. If needed by either side, a government-to-government/executive agreement could be signed by both sides to establish this exchange.*

STEP 3: *Government-to-government/executive agreement to establish a technical exchange working group to develop and agree upon a* ***format for warhead passports*** *to be developed and maintained for each warhead throughout each warhead's life cycle.[14] These should fully represent a unique set of data for each warhead that includes data such as what CNS has identified in this paper. The sides would identify and agree upon each column and precisely how the data shall be entered in each line, representing each time new data on that warhead would be required. The passports for each country may differ so long as they each contain critical, unique data on each warhead. Here is a sample:*

[13] If we are following the precedent of the agreements in START I to have early exhibitions and exchange of data, we should use the Executive agreement format and possibly consolidate all the early actions in a single executive agreement. Alternatively, the sides could have an umbrella agreement and add the details in separate annexes which could be added once agreed. The Appendix to this Annex sets forth a draft agreement on early exhibitions.

[14] Article Two, paragraph 4 of the draft verification protocol.

Date/Time	Location	Status	Secondary Component	Limited Lifetime	Limited Lifetime Component 2	Operation Conducted	Personnel	Nonce Field	Previous Hash	ID Hash
11/13/2017 16:00	CADOL	RP	S01001	LLC101001	LLC201001	R11	AD1			
11/13/2017 17:00	CADOL	RI	S01001	LLC101001	LLC201001	R21	R63S1			
11/15/2017 23:00	WR63S	RI	S01001	LLC101001	LLC201001	R322	R63S1			
11/15/2017 23:30	WR63S	RI	S01001	LLC101001	LLC201001	R23	R631			
11/16/2017 02:30	WA63E	RI	S01001	LLC101001	LLC201001	R25	A637			
11/16/2017 04:30	WA63E	RA	S01001	LLC101001	LLC201001	R16	A637			
05/16/2018 08:00	WA63E	RA	S01001	LLC101001	LLC201001	R43	A632			
11/15/2018 10:00	WA63E	RA	S01001	LLC101001	LLC201001	R44	A639			
05/15/2019 09:00	WA63E	RA	S01001	LLC101001	LLC201001	R41	A633			
11/16/2019 12:00	WA63E	RA	S01001	LLC101001	LLC201002	R45	A634			
05/20/2020 18:30	WA63E	RA	S01001	LLC101001	LLC201002	R47	A632			
11/17/2020 07:15	WA63E	RA	S01001	LLC101001	LLC201002	R41	A633			
05/19/2021 15:30	WA63E	RA	S01001	LLC101001	LLC201002	R44	A638			
10/13/2021 00:00	WA63E	RI	S01001		LLC201002	R46	A633			
11/15/2021 07:15	WA63E	RR	S01001			R46	A634			
12/01/2021 05:50	WA63E	RS	S01001			R12	A632			
12/01/2021 09:00	WA63E	RS	S01001			R26	A631			
12/02/2021 21:30	WR63S	RS	S01001			R313	R63S1			
12/04/2021 00:30	CADOL	RS	S01001			R321	R63S1			
12/04/2021 01:30	CADOL	RS	S01001			R22	AD1			

STEP 4: *Government-to-government/executive agreement to establish a technical exchange working group to develop the* ***processes and procedures necessary for a data challenge.*** *The sides would test these procedures using notional data to develop and test confidence in the process. The sides would also develop, and if possible, agree upon, parameters regarding the implementation and use of data challenges to validate data and verify warhead unique identifiers. The parameters should include the annual frequency of the*

data challenge, the amount and type of data that may be subject to a challenge (e.g. a line of data or maybe one or more data points), and the number of challenges permitted per passport on an annual or life cycle basis.[15]

STEP 5: *Government-to-government/executive agreement to establish a technical exchange working group to jointly develop a* ***zk-SNARK tool*** *that can be used to interrogate data represented by cryptographic unique identifiers.*[16] *Using the notional sample data, the sides will create a series of questions and interrogations that the SNARK tool will perform on the sample data and the sides will work together to validate its performance and security capabilities.*

Once the sides agree to investigate or pursue an agreement specifically focused on warheads, the first step should be meetings of a working group on sensor technology since the results will drive the baseline verification measures. The early identification of what sensors to use, at least with respect to specified items (such as nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, and nuclear warhead transport railcars) is essential to ensure that sensors will “fit” on specified items. Once the sensor technologies are agreed upon (Step 6) and following an exchange of maps (Step 7), the two sides could agree on where sensors would be placed.

STEP 6: *Government-to-government/executive agreement to establish technical exchange working group(s) to* ***identify, develop, and test sensors*** *that would be used to monitor the presence and movement of items within each country’s closed nuclear system. Technical exchanges may be conducted initially at neutral test or training facilities such as the Security Assessment and Training Center (SATC) established by the Cooperative Threat Reduction (CTR) program in Sergiev Posad, Russia and an equivalent site in the U.S. such as at one of the U.S. national laboratories.*

This working group should establish how many on-site data sensor checks may be conducted, and should discuss a quota for such checks, setting a total number per year as well as per sensor and/or per facility. The working group should also discuss whether data sensor checks can/should be conducted at the same time as an on-site inspection, with each counting towards its own quota or not.[17]

Article Nine of the draft verification protocol states that the purpose of sensors is to supplement or corroborate data that is provided in notifications on the movement of nuclear warheads or in other declared data, in notification of changes in the location of nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, and nuclear warhead transport railcars, and to detect the movement of undeclared nuclear warheads and the movement of any of the items specified in this paragraph outside declared areas.

The sides may want to establish smaller subsets of the technical group to focus on specific sensors with experts on the relevant technologies. The set of sensors may be negotiated by the sides, but the following should be addressed:

[15] Article Four and Annex 5 to the draft verification protocol.
[16] Article Five and Annex 6 to the draft verification protocol.
[17] Paragraph 1 of Article Ten of the draft verification protocol contains a placeholder for a quota. It also states that sensor data checks can be conducted at the same time and at the same facility or location as an on-site inspection, but they would count against the numerical limit on data sensor checks for that period.

- Radiation and other sensors to be used during baseline and suspect site inspections to verify the number of warheads at a specific site or validate the absence of any warheads at a facility or location. The procedures for conducting such inspections should be negotiated as well.
- Navigation sensors to be installed in trucks, railcars, and aircraft, and all handling equipment that can record navigation routes, but for security reasons they should do so without the capability to transmit data and without GPS capability. Installation instructions for each transportation mode and each transportation conveyance should be developed and agreed. The sides should determine if installation can/should be done by the host party in a verifiable process or if installation should be conducted by joint teams. Both sides should have the opportunity to examine the sensors to validate their capabilities. These devices must be tamper-proof. The sides would need to provide estimates of the quantity and type of transport conveyances and handling equipment that would be incorporated in the closed system, and if possible, the sides should attempt to reach an agreement listing the applicable conveyances and handling equipment.
- Radiation detectors to be installed within all transport conveyances and at designated and agreed interim transportation locations to detect and record dates/times when a warheads or warheads pass by the sensors while in transit or are placed within those conveyances. The sides should determine whether the sensor capabilities shall include the ability to count separate warheads within the conveyances and when they pass by. These devices must be tamper-proof.
- Radiation detectors to be installed at all facility entry/exit points to detect, record, and if agreed, count warheads that pass by the sensor. If agreed, the sides should also develop, test, and agree on the procedures to install and use cameras (either still or video) to record each instance of a warhead passing by the sensor. If agreed, permanent video cameras may also be developed and agreed to record all traffic passing with dates and precise local times recorded. These devices must be tamper-proof and shall not have the capability to transmit data electronically.
- Tamper-proof sensors that shall act as locks to record the dates/times when they are opened and closed to be placed at all facility entry and exit points, all warhead storage and maintenance facilities and bunkers, as well as the doors/openings of all transport conveyances. This working group would need to coordinate with the working group for Step 7 below (Technical exchange of maps) to ensure the same locations are being used.[18]
- The technical working group should also work out the process for producing, storing, and installing all the sensors. Where should they be produced? How should each side check them for bugs? How should they be stored, and where? How to validate

[18] CNS identified 55 “Red” (Russian) and 15 “Blue” (U.S.) warhead storage, transfer, and assembly/disassembly sites in our representative data base during discussions of the Warhead Tracking System. https://nonproliferation.org/wp-content/uploads/2023/03/web_warhead_verification_demonstration030823.pdf. These did not include all the sites that should be listed for this task.

them before, after, during installation, and then again when the data are gathered during a sensor check inspection?

STEP 7: *Government-to-government/executive agreement to* ***exchange a map or diagram of each country's closed nuclear warhead system.*** *The map shall include geographic locations of warhead storage sites, production and maintenance facilities, transportation transfer points, and transport routes. A second map will also be exchanged showing all production, maintenance, and storage facilities for dedicated nuclear warhead support systems such as mobile and overhead cranes, etc. All transport routes shall include a geographic band of all potential routes from each starting and ending points. In addition, the transport routes shall be listed to include a range and allowed variance (variance allowance shall be discussed and agreed upon during the technical meeting) for the time required to transit each route using the designated transportation mode (vehicle, train, or plane) with starting and ending points.*[19] *This data exchange may also include declared suspect sites, such as conventional munitions storage sites that may be subject to a specified quota and procedures for inspections once the obligations of the treaty and/or the verification protocol begin to apply. For INF, START I and New START, the requirement for site diagrams was based on the need to have them available for the inspections (baseline and other on-site inspections). For the draft verification protocol, these site diagrams would also be used as reference during the emplacement of sensors.*

For this CNS paper, we included all warheads in the inventory under the custody of their respective Department or Ministry of Defense, but did not include those warheads installed on missiles or submarines on alert. The study assumed warheads on alert would be subject to the current New START agreement, but its expiration may occur prior to the beginning of the warhead treaty. Therefore, this working group should address the question of whether to include warheads on alert in the closed warhead system by adding or including these additional locations and routes. They should also address how alert warheads should be treated in a potential future warhead limitation agreement.

STEP 8: *Government-to-government/executive agreement to develop the processes, procedures, and exact* ***placement of specific sensors*** *on specific pieces of equipment for both sides. From the results of Step 6, this working group should address each piece of equipment, including support equipment such as cranes and forklifts, transportation systems, including the route sensors, radiation detection, and door opening sensors, as well as detection equipment to be placed along transport routes, should be developed, defined, and agreed. The processes and procedures should address the personnel required/permitted and any support equipment needed for the placement, calibration, and testing of individual sensors.*

The final steps would be agreements laying the groundwork for traditional verification and inspection activities: open displays and technical demonstrations, suspect site inspections, and on-site inspections.

STEP 9: *Government-to-government/executive agreement to establish technical exchange working group(s) to conduct technical exchanges on* ***open displays[20] and technical***

---

[19] Article One, paragraph 5 of the draft verification protocol.
[20] Article One, paragraph 5 of the draft verification protocol.

demonstrations[21] *that may be required to support any of the working groups above. These should include exhibition/technical demonstration/open displays of all items that are to be subject to inspection, to ensure the effectiveness of the baseline inspections.*

Technical Characteristics Exhibition: The draft verification protocol provides that the technical characteristics exhibition shall be conducted after signature.[22] Without an exhibition of the technical characteristics of all items subject to inspection, to confirm their appearance and dimensions, it is not clear how effective an inspection would be if the purpose of the inspection is to verify the presence or absence of such items. The technical characteristics exhibition should be conducted within a number of days after signing the separate agreement on the technical characteristics exhibition, or at some point prior to the signature of the treaty, or at some point prior to entry into force of the treaty of the warhead agreement, to ensure the effective conduct of the baseline inspection regime.

There is a precedent for a technical characteristics exhibition prior to entry into force of the primary agreement: it was done through a separate agreement on early exhibitions in START 1, in order to facilitate implementation of the inspection regime once the treaty entered into force. A proposed draft of such a separate agreement, based on the START I precedent, is set forth in the Appendix to this Annex.

STEP 10: *Government-to-government/executive agreement to identify sites to be designated for* ***Suspect-Site Inspections (SSIs)*** *and to establish criteria and procedures for conducting SSIs at designated and non-designated suspect locations. The sides should discuss, in great detail, the intertwined issues of intrusiveness, verifiability, and negotiability in connection with an SSI regime. Issues include the criteria for a facility or site being subject to SSI, the appropriateness of the time limits in the SSI regime, and quotas.*[23]

STEP 11: *Government-to-government/executive agreement governing* **On-site Inspections (OSI)***. The sides should discuss when the right to request an OSI begins, the quotas for such inspections, and the requirements for a baseline OSI.*[24] *They should also negotiate the number of OSI per year, and the number of such inspections for a specified facility or location.*[25] *The sides should also discuss whether the time limits identified in Annex 7 (paragraphs 1, 2, and 3) of the draft verification protocol concerning the conduct of OSI are appropriate, perhaps in reference to the time limits specified in INF, START I and New START, and whether/why the inspection procedures, borrowed from those earlier treaties, are appropriate for the warhead agreement. They should also address the purposes of OSI in the Verification Protocol and whether they are reasonable, negotiable, and important for monitoring compliance over time.*

For each of the steps listed above, a preliminary step could be added to conduct such exchanges using notional or representative passports and data. CNS developed 25 realistic passports for a Red and a Blue country that could provide a starting point for such exchanges.[26]

[21] Article Thirteen and Annex 14 to the draft verification protocol.
[22] Article Thirteen, paragraph 1, and Annex 14, paragraph 1 to the draft verification protocol.
[23] Article Eight and Annex 9 to the draft verification protocol.
[24] Baseline OSI was not included in the draft verification protocol.
[25] Paragraph 1 of Article Six of the draft verification protocol has placeholder for quotas, as well as for limitations on the number of OSI at a specified facility or location.
[26] https://nonproliferation.org/wp-content/uploads/2023/03/web_warhead_verification_demonstration030823.pdf

All of the steps described above that involve the exchange of cryptographic software, hardware, and all sensors would be subject to export control reviews to allow them to be implemented in each country.

Ideally, we would establish estimated timelines for each of the above, but there are so many variables at play in establishing a step-by-step process that no estimates would be reliable. It would not be unreasonable to anticipate that completing all of these steps would require at least 1-2 years to accomplish, perhaps 3 for the teams to thoroughly investigate each step. Political support would be needed throughout this process, with each agreement identified as a sign of progress.

B. ENHANCED VERIFICATION MEASURES

1. Baseline Activities to Begin Upon Signature of the Treaty and/or the Verification Protocol

After all or most of these preparatory or preliminary steps are completed, the sides would be prepared to jointly develop a complete agreement to exchange warhead data, which could be part of (or precursor to) an agreement on warhead limitations (should one be desired), a transparency regime without specified limits, and/or part of its verification protocol. Baseline activities could begin at signature of one or both of the two legal instruments rather than entry into force (which could take a long time). As noted above, the verification protocol could be negotiated separately and its provisions could begin to apply at signature, but it would likely be considered to be an integral part of the agreement upon entry into force. The major question is whether that would be acceptable to both sides - if the verification regime is not yet agreed, would or could there be a legally binding agreement on maximum numbers of warheads?

In any event, once the obligation to provide data begins,[27] the data would be exchanged in the form of a ledger of cryptographic commitments representing each warhead in each country's inventory subject to the agreement.

From these preliminary and preparatory steps, the sides would hopefully have developed mutual confidence in the processes, procedures, and data required to reach consensus on an agreement that could freeze or place other limits on their respective nuclear warhead stockpile. The substance of any such agreement shall include the outcomes of the preliminary steps above and the draft verification protocol – which may require some modifications based on these preparatory steps.[28]

In addition, the sides would need to develop and agree upon a process to establish and verify the baseline of declared data. The draft verification protocol included procedures on providing data to establish a baseline but did not develop a specific baseline verification procedure that would allow verification of all the declared data, and, in particular, did not

[27] Article One, paragraph 1 of the draft verification protocol includes a placeholder for time period following signature of the protocol.

[28] The draft verification protocol was not modified to incorporate these enhanced verification measures.

develop procedures for a baseline OSI regime. However, some ideas on baseline verification measures are provided in the next section of this Annex. This issue could also be discussed via a technical exchange or could be the first step in a final agreement negotiation addressing the results of the preliminary steps and the application of those steps to the draft verification protocol.

With these considerations in mind, the first official step after the obligations of the final agreement and/or verification protocol begin to apply should be the technical exchange of the following:

1. Cryptographic Ledger of all warheads defined within the agreement containing all required data for all warhead passports updated to the exact date of the agreement and initial date of a no-movement period.
2. Unless provided earlier under a separate agreement, closed system maps, including a listing of all facilities, all allowable routes depicted geographically and by travel time ranges, and transfer points. The maps and facility diagrams shall identify the proposed sensor emplacement locations.[29] The listing should be updated if it was provided earlier during a technical exchange.
3. Each side shall exchange a proposed schedule for joint installation of all sensors unless a preliminary agreement included earlier emplacement of sensors.

All warhead movements, including all support equipment movements, shall be prohibited for a certain period of time[30] after the obligations of the treaty and/or the verification protocol begin to apply (unless a different amount of time is agreed). This time shall allow for joint sensor emplacement and/or on-site sensor inspections, on-site inspections, and suspect site inspections as agreed. The on-site sensor inspections will not be necessary if all sensors are jointly installed prior to signature of the treaty and/or the verification protocol. In this case, however, the sides shall agree on a specific number of random on-site sensor inspections (maybe 25% or 33% . . .) to validate the installations and to monitor the no-movement period.[31]

2. Baseline Verification Measures

The next important question is how we verify the baseline data. The no-movement period will be critical to establishing confidence in the initial data declarations.

Unless the sides have already installed all the sensors establishing the closed system and all equipment within the closed system, then the first baseline activity will be to install all of those systems as agreed during the preparatory technical exchange. Unless agreed otherwise, this shall require joint on-site visits to all declared locations and shall include a methodology to account for the location of each declared warhead identified in the exchanged ledger of cryptographic

[29] Article One, para 3 and 4 of the draft verification protocol.
[30] The time period would be based on an analysis of the number of teams, number of personnel, and time required to install all sensors and conduct a baseline inspection.
[31] The no-movement requirement is not included in the draft verification protocol, but was subsequently identified by CNS as providing an important addition in order to effectively verify the baseline data. All of the baseline verification measures identified in this section of the Annex flow from that determination.

unique identifiers. Teams could conceivably be as small as a four people,[32] with a team lead, two technicians to operate the equipment and record the results, and an interpreter.

There are 10 types of facilities/areas that would need to be visited and/or inspected if all such facilities were subject to baseline verification measures. Depending on the outcome of the technical exchange on the applicable sites within the closed system, the sides should provide the number of each type, as well as to provide the applicable site names – this data would also be relevant for other types of on-site activities, including OSI:

(a) nuclear warhead storage facilities;

(b) nuclear warhead production/disassembly facilities;

(c) road-rail transfer points;

(d) rail transfer points;

(e) air transfer points;

(f) loading and unloading locations;

(g) nuclear warhead transport vehicle secure storage/parking areas;

(h) nuclear warhead transport railcar secure storage/parking areas;

(i) nuclear warhead air transport secure parking areas; and

(j) nuclear warhead container storage locations.

Assuming that baseline OSI is included among the baseline verification measures, ideally each team could also conduct the required baseline inspection(s) at each site as they install all of the sensors. If each facility were to require between 10-24 hours for a thorough inspection, then one team could probably examine 2 or more sites per week. Depending on the number of sites identified within each country's closed warhead system,[33] the baseline inspections would require at least 6 teams of 4 persons (each team working 2 weeks on and 2 weeks off) to accomplish all required baseline inspections in the no-movement period.

Simultaneously with the on-site baseline inspections, each side shall also conduct additional validation efforts within this no-movement period in order to correlate the data collected on-site with the submitted cryptographic data:

- The sides shall also execute an agreed number and type of open displays and technical demonstrations during the baseline period.[34] For example, the sides could require specific handling equipment, such as one or more mobile cranes, to be displayed in the open for a specific period (such as two days) within each site immediately following completion of the baseline inspection at the site. Technical

[32] Under the CTR program, 4 person teams were granted access to Russian warhead storage facilities for 4 hours to validate completion of installation work on nuclear security systems.

[33] The numbers of sites identified during the demonstration of the warhead tracking system, 55 Russian, and 15 U.S., should be considered lower bounds on the number of sites that may be subject to baseline inspections.

[34] Article Twelve of the draft verification protocol does not include the obligation to conduct open displays during the baseline period; instead, there is a placeholder for quotas. Article Thirteen requires the parties to conduct a one-time technical characteristics exhibition of each type of its nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear security equipment, nuclear warhead transport vehicles and nuclear warhead transport railcars. There is a placeholder for the time period during which such exhibition must be conducted.

demonstrations of other handling equipment, such as overhead cranes, could/should be conducted during the baseline inspections at each site.

- The sides shall execute an agreed number of data challenges within this no-movement period. These data challenges can/should be correlated with specified open displays during this period to help validate the overall cryptographic database. At least one data challenge per warhead passport shall be executed and validated during the period.[35]
- The sides shall execute an agreed number of zk-SNARK interrogations, including one conducted upon signature to validate the initial ledger, and one per __________ until the end of the no-movement period.[36]
- The sides shall execute an agreed number of Suspect Site Inspections during this no-movement period to detect potential misplacement of any warheads outside the designated closed system. Ideally, this shall include all declared and pre-identified suspect sites as well as any other sites of concern.[37]

3. Annual Validation Activities and On-site Activities to be Implemented After the Obligations of the Treaty and/or the Verification Protocol Provisions Begin to Apply

After the obligations of the treaty and/or the verification protocol begin to apply and after the completion of the baseline period, further regular verification measures shall be conducted in accordance with the verification protocol. These shall include:

- Specified notifications of movements (as agreed)[38] and updated cryptographic commitments for each warhead passport subject to any agreed transaction.[39] Depending on the results of the technical working group(s) these notifications may be provided one at a time at a time designated by the working group following the actual movement, or they may be provided in batches per week, month, or quarter.
- An annual quota on data challenges, including a quota on the number of challenges permitted per warhead and per facility or location.[40]

[35] Article Four of the draft verification protocol does not include the requirement for data challenges during the baseline period or the requirement that at least one data challenge per warhead passport be executed and validated during the baseline period.
[36] Article Five of the draft verification protocol does not include the requirement for zk-SNARK interrogations during the baseline period.
[37] Article Eight of the draft verification protocol does not include the requirement for suspect-site inspections during the baseline period.
[38] Paragraph 6 of Article One of the draft verification protocol contains a placeholder for the time period - these notifications apply to movement of nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, and nuclear warhead transport railcars to another facility or location. The movement of nuclear warheads is notified separately, in accordance with Article Three and Annex 4 to the Protocol.
[39] Paragraph 5 of Article Two of the draft verification protocol contains a placeholder for the time period.
[40] Article Four of the draft verification protocol includes a placeholder for the number of data challenges permitted for each Party. Paragraph 1 of Article Four states that "[t]he amount of data to be revealed in each data challenge, the timelines for responding to data challenges, and the methodology used to determine how the amount of data revealed in a data challenge applies to the quantitative limits on data challenges, shall be agreed between the Parties."

- An annual or monthly quota on zk-SNARK interrogations that may include sub-quotas on specific types of interrogations (validating data entries vs. verifying the time involved in specific transportation activities or verifying sensor data that should match passport data for example).[41] For example, a monthly zk-SNARK interrogation may confirm and validate the status of the cryptographic database.
- Annual quota on Suspect Site Inspections (subject to quota on On-site inspections).[42]
- Annual quota on On-site sensor inspections.[43]
- Annual ledger exchanges and annual updates of all maps and routes.
- An annual quota on On-site inspections.[44]
- Close-out inspections. The time limits in the close-out inspection regime[45] and specific close-out procedures will need to be negotiated based on precedents from other treaty regimes, as well as DTRA/CTR experiences.

The closed system approach that uses sensors at all entry and exit points for the closed system and for each facility/location, along with sensors installed on the handling equipment and with cryptographic passports representing location and logistics data for each warhead provides tools to triple check all data within the closed system. The passport data, the handling equipment data, and the entry and exit point data can all be correlated through data challenges and through the use of zk-SNARK interrogations as well on on-site inspections. The use of data challenges and zk-SNARK interrogations supplement on-site inspections in terms of increasing verification capabilities. As confidence in the system grows over time, this could enable a reduction in on-site inspection requirements.

4. Bilateral Verification Commission

During all of the baseline and annual verification activities, any/all issues shall be raised to the Bilateral Verification Commission if not resolved within a specified period of time.

[41] The draft verification protocol does not include any quotas (Article Five and Annex 6)
[42] Paragraph 2 of Article Eight of the draft verification protocol states that each suspect-site inspection shall reduce the number of on-site inspections to which the inspecting Party is entitled by one for that period.
[43] Article Ten and Annex 11 of the draft verification protocol.
[44] Paragraph 1 of Article Six of the draft verification protocol contains a placeholder for the quota, as well as a placeholder for the number of inspections at a specified facility or location during that period.
[45] Annex 8 of the draft verification protocol.

Annex E. Cheating Scenarios

These scenarios describe how the other party may seek to violate the agreement and avoid detection, as well as show the ways that the overall closed system and its various verification measures could be used to deter, detect, and identify the two specific cheating scenarios. For purposes of this Annex, CNS will assume that the enhanced verification measures identified and described in Annex D are in place.

This Annex will address two of the most concerning and serious cheating scenarios:

Scenario 1: One country may produce new warheads that are not declared and are handled completely outside of the closed system. This scenario will also address the risk that a certain number of warheads will be located outside the closed system at time of the baseline and remain undeclared.

Scenario 2: One country may piggyback one or more warheads along with a declared warhead(s) and within the closed system. It would not declare one or more and operate it (them) within the system for its (their) entire service life without detection.

Each of these scenarios will be assessed by:

- describing the actions we would take that would either preclude or detect the violation(s),
- addressing the risk of unsuccessful detection and
- quantifying that risk (e.g. they might be able to keep a handful out of control, but not a significant quantity).

Scenario 1: Production of New/Re-furbished, Undeclared Warheads

Under this scenario, the primary verification measures to prevent or detect warheads outside of the closed system would be Suspect Site Inspections (SSI)[46] and detection by National Technical Means of Verification (NTM) of the transportation means and equipment used around the production facilities and surrounding the closed system.

During the baseline period, each side shall have the right to inspect suspect sites, thus deterring and preventing the opportunity that the other side would be able to hide nuclear warheads within those facilities during that period.[47] According to the draft verification protocol, each side has the right to conduct suspect-site inspections at facilities and locations where nuclear warheads, nuclear warhead containers, nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles or nuclear warhead transport railcars have not been declared or notified but regarding which a side has concerns about the possible presence of such items.[48] The types of facilities and locations subject to suspect site inspections are not restricted to those within the "closed system" and include those

[46] Article Eight and Annex 9 of the draft verification protocol.
[47] See Annex D on enhanced verification measures during the baseline period.
[48] Article Eight, paragraph 1 of the draft verification protocol.

that (a) have a characteristic signature of a nuclear weapons storage facility or (b) possess containers large enough to contain a nuclear warhead, and possess support equipment, vehicles, or railcars similar to those present at the facilities and locations listed within the "closed system" in the draft verification protocol.[49]

The sides have (at a minimum) two opportunities to detect these undeclared warheads during an SSI: during the baseline period, or during subsequent SSI inspections (subject to quotas). For the former, each side would have its own list of facilities and locations that meet these criteria at the time of the baseline period. For the latter, the decision on whether to conduct an SSI would be made during the implementation of the agreement. The sides also may agree on additional facilities and locations that would be subject to suspect-site inspections,[50] but it is unlikely that they would be used in a cheating scenario because of the near certainty of detection, at least not during the baseline period.

With respect to detection by NTM, the technical characteristics exhibition is crucial in ensuring the effectiveness of NTM in detecting undeclared nuclear warheads and their movements. During the exhibition, each side must exhibit its nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, nuclear security equipment, and nuclear warhead transport railcars.[51] In addition, to ensure more effective on-site inspections (OSI), the exhibiting side must point out the external differences that distinguish any of these items from similar items used for activities related to the storage, handling or transport of conventional warheads,[52] and shall allow the other side to take measurements to confirm the technical data for recognition of that item during a potential OSI.[53] Based on this exhibition, which represents each side's agreement to use only these transportation means and equipment for both nuclear and/or conventional warheads, a side wishing to evade detection would either (a) have to construct a totally new fleet of vehicles with different configurations and measurements, as well as new types of warhead handling equipment, and it would use these new items to transport and handle nuclear warheads outside of the closed system, or (b) ensure, through intricate planning and scheduling, that all transportation of these undeclared nuclear warheads using previously exhibited vehicles and equipment was conducted at times and places that NTM would not be able to detect their movement or activity, such as during inclement weather, at night, or in an area that was not under continual monitoring by NTM. In addition, each side will want to be aware and utilize all NTM to look for trucks capable of transporting warheads and warhead handling equipment outside the suspect sites prior to the baseline period and to look for the return of any such trucks after baseline.[54]

Within this scenario, another thing that the cheating party could attempt would be to keep a certain portion of its warheads undeclared, as a "shadow stockpile" while pretending to comply with the data exchange and on-site inspection regime by providing data and notifications for the other portion of its warheads, and receiving inspection teams, in

[49] Annex 9, subparagraphs 3(a) and 3(b) of the draft verification protocol.
[50] Annex 9, subparagraph 3(e) of the draft verification protocol.
[51] Article Thirteen, paragraph 1 of the draft verification protocol.
[52] Annex 14, subparagraph 4(b) of the draft verification protocol.
[53] Annex 14, subparagraph 5(b) of the draft verification protocol.
[54] There is a prohibition on warhead movement during the baseline period in Annex D, although the amount of time has not been specified, pending further analysis.

accordance with the Verification Protocol. This scenario would also require constructing new, undeclared facilities to maintain the shadow stockpile entirely outside the closed system. But such an attempt would be difficult to sustain because construction activities could be detected and attributed via NTM and SSIs. The equipping of the undeclared facilities could also be detected by NTM and by sensors and potential OSI of equipment production facilities. These facilities would also require maintenance capabilities and trained personnel, thus increasing the probability of detection.

Moving one or two warheads would be difficult to detect but trying to move more than one or two AND moving and using the required handling equipment would be extremely difficult to execute without detection by NTM.[55] It would likely require extensive efforts such as digging new underground passageways to escape detection of such operations. The problem with that would be that digging underground caverns is extremely difficult to do without detection by NTM, and even if they could be built without detection, they would have to escape detection for the duration of the agreement. If underground detection equipment were included on the suspect site inspection equipment list, this would be doubly difficult. Therefore, equipment such as ground penetrating radar is included in the draft verification protocol.[56]

The inclusion of warhead handling equipment in the closed system regime also makes this scenario more difficult to carry out without detection because such equipment movements not consistent with the procedures in the agreement would increase the risk that such movements and activities would be detected.

This scenario also accentuates the importance of installing nuclear detection sensors/monitors at all exit/entry points at all nuclear warhead production facilities.[57] Once again, the cheating scenario could be executed by building covert underground transportation pathways, but these are subject to detection through NTM and the use of underground cavern detectors.[58] The key would be to ensure that all possible entry/exit points of the production facilities are captured by nuclear sensor/detectors that are enclosed with strong intrusion detection capabilities.[59] Having that equipment in place would not prevent a warhead or warheads from exiting the facility without declaration, but once the equipment data are collected any attempts to move warheads in a non-declaratory manner would be recorded. Attempts to alter the sensors would be deterred and detected by the intrusion detection capabilities.

---

[55] If we assume, hypothetically, that the chance of detecting a covert single-warhead transfer is 5%, then the cheating side still has decent chances of avoiding detection after several more transfers. But, after 14 covert transfers the probability of avoiding detection of any single transfer decreases below 50%. Extending such probabilities over the lifetime of an undetected warhead and all of the actions required to maintain undetected warheads the probability of detection increases dramatically and the probability of continued success by the cheating party drops significantly. See the Appendix to this Annex for a more thorough explanation.

[56] Annex 7, subparagraph 14(c) of the draft verification protocol. Paragraph 6 of Annex 9 provides that SSI inspection teams shall have the right to use the inspection equipment provided for in paragraphs 13 and 14 of Annex 7.

[57] The obligation to install sensors at nuclear warhead production/disassembly facilities is provided for in Article Nine, paragraph 1, and in Annex 10, subparagraph 1(d) of the draft verification protocol.

[58] On the assumption that an OSI could be conducted at a production facility – the draft verification protocol does not exclude that possibility.

[59] Annex 10, paragraph 7 of the draft verification protocol provides that all sensors to be emplaced shall be equipped with tamper-proof seals.

The cheating party could attempt to take undeclared nuclear warheads out of the closed system by exercising its right to move nuclear warhead support equipment and vehicles, nuclear warhead transport vehicles, and nuclear warhead transport railcars for maintenance or repair to a facility or location other than those listed in the draft verification protocol, but this right is limited to an "exceptional basis" requirement, and notifications must be provided before its departure and following its return.[60] Thus, its movement would be known in advance and subject to detection by NTM or by a subsequent SSI of the maintenance or repair facility or location.

Since the sensor/equipment data would only be collected during an on-site inspection or an on-site data sensor check,[61] detection of such activity could be delayed until such an inspection or data sensor check was conducted. Such time delays could be mitigated through more frequent on-site inspections or data sensor checks, or through SNARK Tool interrogations if the host party were required to gather and enter the data on a more frequent basis. Special procedures would be required such as real-time video of the data collection activity. These overlapping capabilities would serve to deter illegal production of new or refurbished, undeclared warheads and detect such activity if the host party ignores their agreement commitments.

Finally, this scenario would also need to address the probabilities and risks of a cheating party to move warheads in and out of the closed system along transport routes or at transfer points. One of the best ways to monitor activities along these routes would be to use SNARK tool interrogations that would ensure that all movements comply with required/declared travel times, and routes and transfer points which would be recorded by verification sensors.[62] Since all transport and handling equipment would be sensored, any anomalous use of that equipment would be detected upon sensor data collection activities so long as the sensors were carefully protected against intrusions. Even the use of non-declared handling or transport system would be detected at any/all entry, exit, or transport route checkpoints.

These multiple capabilities, which overlap each other and create layers of protection, greatly increase their deterrence strength and detection probabilities. Efforts by the host party to surreptitiously deploy non-declared warheads would need to be extensive to hide even one or two warheads and would make it extremely difficult to hide a significant quantity.

Scenario 2: Operating Undeclared Warheads Within the Closed System

The second cheating scenario that could be considered by a party wishing to hide warheads outside of an agreement would be to maintain a certain number of undeclared warheads within the closed system.

This scenario would probably be quite difficult on the U.S. side due to the much smaller number of facilities within the closed system. The Russian side, on the other hand, would likely have to declare numerous storage sites, rail transfer points, and even multiple

[60] Article One, paragraph 8 of the draft verification protocol.
[61] Article Ten and Annex 12 of the draft verification protocol.
[62] Article Nine of the draft verification protocol obligates the sides to install sensors along routes and at transfer points, but the cheating party could attempt to circumvent detection by deliberately avoiding the emplaced sensors, although the declared travel times would make such an attempt highly risky.

production facilities. The high number of facilities creates challenges to identifying and detecting potentially undeclared warheads hidden within those facilities.

Of course, baseline inspections of each of the Russian declared facilities and the installation of sensors to enclose the system while there is a moratorium of warhead movements will be key to deterring any such activities. Since warheads are so mobile, a cheating party could try to move warheads within facilities during an on-site inspection in such a way that the inspecting party may have difficulty in detecting an undeclared warhead. Hand-held nuclear monitors with appropriate procedures in the verification protocol could help prevent such activities.[63] It would also be important to use all NTM resources possible to monitor the facility during a baseline inspection to detect anomalous behaviors and movements of warheads AND any non-declared handling equipment that would be required for such movements. Subsequent OSI of these facilities and on-site sensor data checks would also increase the chances of detecting non-declared warheads or handling equipment. The cheating party could not use declared and monitored handling equipment to move and maintain non-declared warheads, thus requiring them to hide that equipment as well within the closed system.

A cheating party could attempt to hide undeclared warheads within transport containers that also contained declared warheads to conduct required maintenance and safe handling and storage of non-declared warheads. Such an attempt would easily be detected within the transportation systems if those systems were equipped with nuclear detection equipment capable of differentiating the nuclear signals in such a way that the warheads could be counted. The risk of detection during routine OSI conducted at storage and transfer facilities would be high so long as the verification protocol were to restrict movements prior to and during OSI[64] and as long as the inspection party were to be equipped with handheld equipment that enabled the detection and counting of warheads within a facility.

We should note that, in the draft verification protocol, on-site inspections may not be conducted during warhead transfer operations,[65] and this carve-out may give an opportunity for a side to cheat by transferring or swapping out undeclared warheads. But that provision also provides that the facilities and locations at which warhead transfer operations are being conducted shall be identified to the inspection team at the time of its arrival at the point of entry, so there may be an opportunity for the inspection team to alert its national authorities of this activity at that facility or location. This information could result in subjecting that operation to some contemporaneous NTM monitoring or at least in identifying that facility or location for an OSI once the warhead transfer operation is completed.

When you combine baseline inspections, OSI, and sensor collection activities you create a high probability of detecting undeclared warheads within the closed system. Especially if the inspecting party cleverly employs the zk-SNARK tool to ensure all equipment is being used as declared and that there are no anomalies in behavior.

[63] Annex 7, paragraph 14 of the draft verification protocol provides for the use of such equipment during OSI.

[64] Annex 7, paragraph 2 of the draft verification protocol establishes pre-inspection movement restrictions at the inspection site: during that time, containers, support equipment, vehicles, and railcars large enough to contain a nuclear warhead and covered objects large enough to contain or to be such items may not be removed from the inspection site.

[65] Article Six, paragraph 3, of the draft verification protocol.

The best scenario for a country to hide warheads within its closed system would be to have undeclared warheads piggyback with one or more declared warheads in such a way that their passport history was essentially identical to a declared warhead. In this way, every movement would be conducted with one or more extra warheads. This scenario would be complex, but not impossible to implement if the inspecting party never had equipment capable of counting individual warheads or if such equipment would be susceptible to counting two warheads as one. This is why it would be important to have nuclear detection equipment that can discern unique warhead signatures.

Once again, for this scenario, multiple overlapping verification measures would deter potential cheating attempts by creating a high probability of detection. The probability of detection increases substantially due to the length of time that a non-declared warhead or warheads would have to be maintained and operated within the closed system without detection. Some facilities are so large and extensive that it is not impossible to imagine that a handful of warheads could exist within the facility undetected, but once the cheating party tried to move them, the probability of detection would increase further. Thus, the cheating party would need to calculate the benefit of hiding a handful of warheads against the risk of detection and noncompliance with the agreement. The benefits would be small, but the risk of reaction by the other side could be substantial depending on the extent of the detected violation.

ADDITIONAL THOUGHTS AND CONSIDERATIONS

As potential cheating scenarios are being evaluated, it is also important to consider the potential strategic significance of the cheating. While moving one or two warheads would be difficult to detect, but unless the number of warheads were reduced to a number much smaller than current stockpiles, one or two warheads may have no significant impact on strategic stability. So long as the verification regime greatly increases the probability of detection as the number of warheads increases, then the protocol should be considered as achieving its strategic objectives. In sum, cheating on a small number of warheads is unlikely to be significant, but cheating on a large number of warheads is likely to be detected. Although cheating on a small number of warheads once or twice and remaining undetected may be feasible, the probability of detecting any individual cheating attempt will eventually become likely as the number of those attempts grows. The rate at which the probability of detection grows would depend on the confidence threshold for detecting an individual cheating attempt. For example, if a covert transfer of a single undeclared warhead has a 5% chance of being detected, after 14 such transfers the cheating side will run a risk greater than 50% of getting caught. Thus, there would be diminishing returns for the cheater.[66]

[66] During our early discussions with Dr. Martin Hellman of Stanford on the warhead tracking system, he stated that "If a fraction X of the data has been faked (e.g., there's really nothing there), after N challenges the chances of the fake not being detected is (1−X)N. For example, if 10% of the data is faked and you have 20 challenges, the chance of NOT detecting the fake is 0.920= 12%. Put differently, there would be an 88% chance of detecting the fake. The "faker" probably wouldn't be willing to risk even a 10% chance of being found out." If you were to extrapolate this math over the lifetime of a warhead, consider all the activities required to maintain a warhead outside of a closed system, and the multiple layers of checks involved in the warhead tracking system, it is clear that cheating would be subjected to increasingly diminishing returns over time.

Another point is that while there may be lots of ways to cheat, but if the sides were to agree on the concept of a closed system and put it in place, additional more complex cheating scenarios are unlikely to achieve significant advantages in a closed system. A key reason is that the warheads are continuously tracked during their entire lifecycle and using a SNARK tool to evaluate and monitor behavior over the course of the entire agreement greatly reduced opportunities for anomalous behavior. Consider just one example, decoy warheads in the closed system, warheads that are not real but have the same signature as real warheads (the old template problem). These could at the least seem to extend the stockpile more than what it is, but not significantly. Another example is switching warheads with different statuses, but this would also be detected even if the retirement facility is outside of the closed facility. Similarly, a state could attempt to delay the declaration of warhead status changes, moving warheads out of the closed system under the guise of retirement, but the discrepancies in timelines or suspicious movements would likely trigger detection. Another potential method might involve manipulating warhead passports to relocate warheads to areas that may be more difficult to monitor within the closed system, yet the robust cross-verification and inspection protocols would make this a high-risk, low-reward strategy. Lastly, tampering with sensors to mask warhead movements could theoretically allow for unauthorized activities, but the chances of successful long-term evasion are slim due to the redundancy and integrity checks built into the verification system. None of these methods have strong incentives for the cheater. So there is no large reward for the cheater and so the risk may not be worth it.

One possible cheating scenario which is quite hypothetical, is just as we use sophisticated techniques to catch cheating the cheating party could use sophisticated techniques to avoid cheating to be detected. For example, if the cheater wants to manipulate the passports/sensors in some way for an ultra-complex cheating scenario they could use sophisticated algorithms, game theory, and AI to minimize the probability of cheating being detected and optimize not being caught. The assumption in the first paragraph of this section is that a lie will always catch up with you, but truthfully that depends on how good you are at lying! States may have sophisticated models that just like in the game of “Go” can game out all the possibilities to be caught and find the best way to cheat but not be caught. This increases the reward-to-risk ratio. This is also why in an actual system it is the role of the other party to constantly look for patterns in behavior using similar sophisticated models for detecting cheating in the data of warhead movements.

Additionally, in the event of catching an attempted violation, the detecting party should immediately apply its new knowledge of the cheating practice to its past observations of the cheating party’s behavior, so that it may determine whether there have been similar undetected violations in the past. If the inspecting party catches one single-warhead movement and assumes that this is the only violation, the other covert movements in the series would remain undetected, and the reaction might not be commensurate to the actual scope of the cheating, especially if the cheating party can successfully argue that there was an emergency/etc. This is why it is so important for the cheating party to fully investigate any/all anomalous activities and use the multiple layered tools provided by the closed system and warhead tracking system.

APPENDIX: RELATIONSHIP BETWEEN PROBABILITY OF DETECTION AND NUMBER OF CHEATING ATTEMPTS AFTER WHICH DETECTION BECOMES LIKELY

For a given probability X of detecting any single cheating attempt (e.g. a covert transfer of one or two warheads), the probability of detecting a cheating attempt when there are Y consecutive attempts is $P=1-(1-X)Y$.[67]

If we define "likely" as "above 50%," then the probability of detecting at least one small cheating attempt out of a series of attempts is likely when. This means that we can solve for the number of Y cheating attempts as a function of the capability of detecting cheating X as:

Returning to the example in Scenario 1, if the probability of detecting a single small-number warhead transfer is X=5%=0.05, then the number of such transfers after which detection of at least one of them is above P=50% is

$$Y=log0.5log(1-0.05)=13.51\approx14$$

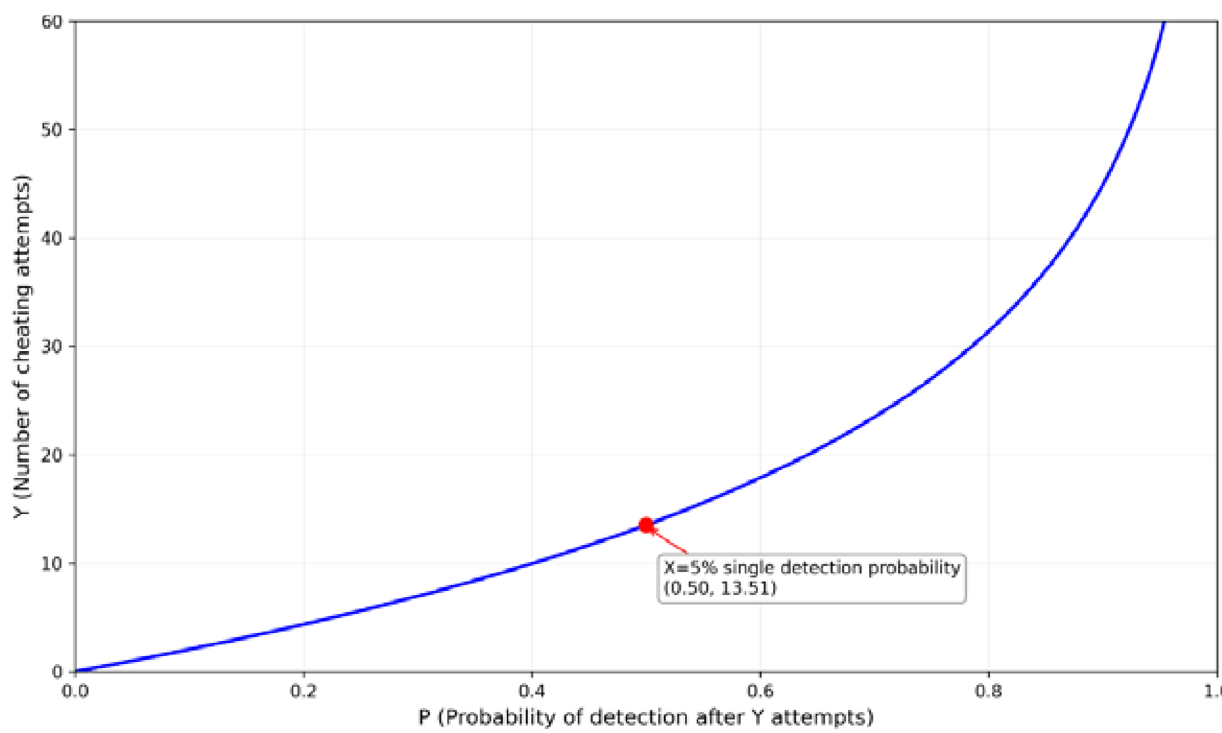

Figure 1: This graph illustrates how the number of cheating attempts (n) increases as the overall probability of detection (P) rises, given a constant 5% chance of detecting any single attempt. The curve demonstrates the non-linear nature of this relationship, with n increasing more rapidly as P approaches 1. The point (0.50, 13.51) is highlighted, showing that approximately 14 attempts are needed for a 50% overall chance of detection when the single-attempt detection probability is 5%.

[67] National Research Council. 2005. *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities.* Page 62-65. Washington, DC: The National Academies Press. https://doi.org/10.17226/11265

To be sure, the actual probability of detecting a single cheating attempt will depend on the magnitude of the cheating scale and the methods used by the cheating party to obscure the attempt and by the detecting party to monitor compliance. The relationship between a given probability and the number of cheating attempts after which the threshold of detection crosses 50% is visualized in Figure 2 below, with our specific example plotted on the graph.

Y vs X for P = 0.5

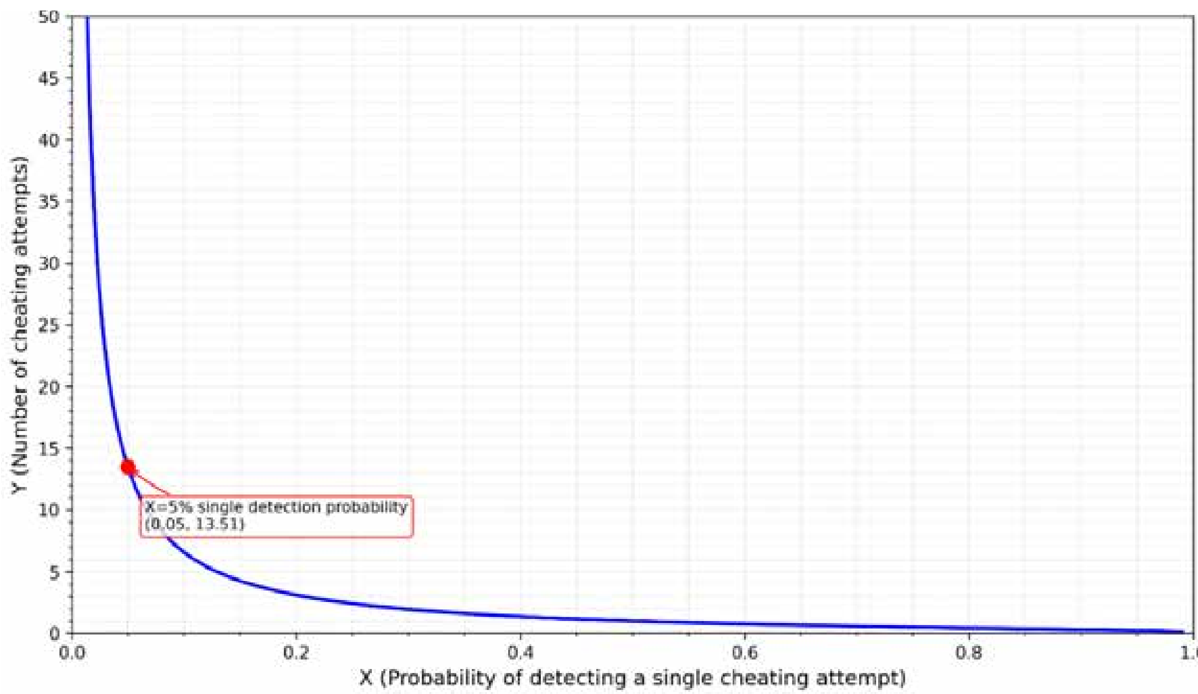

Figure 2: This graph illustrates how the number of cheating attempts (Y) decreases as the probability of detecting a single attempt (X) increases, given a fixed 50% overall detection probability (P = 0.5). The curve demonstrates the non-linear nature of this relationship, with Y decreasing rapidly as X increases, especially for lower values of X. We see that approximately 14 attempts are needed for a 50% overall detection probability when the single-attempt detection probability is 5%.

The curve in Figure 2 represents the threshold number of attempts after which the cheating party runs the likely risk of being discovered. A point below the curve may be deemed relatively “safe” for the cheating party, while a point above the curve may be deemed “unsafe” because of larger risk of detection. This figure reinforces what was stressed in “Additional Thoughts and Considerations:” the cheater will gain diminished returns from consecutive cheating when balanced against the risk of detection. Since, as the cheating party increases the number of attempts, they get closer to (and eventually cross) the threshold where detection becomes likely. This means that each additional cheating attempt brings them closer to detection, offering diminishing returns in terms of successful cheating versus the risk of being caught.

This analysis, however, overlooks two crucial factors that affect the cheater’s decision-making process. First, it doesn’t account for the benefits the cheater actually gains from successful cheating attempts, which would influence how many times they choose to cheat. Second, it assumes the cheater knows the exact probability of being caught on a single attempt (X), when in reality, this value is likely unknown to them beforehand. Without this knowledge, the cheater would need to act more conservatively to avoid detection if that is of paramount importance to them, further reducing the potential gains from cheating. These limitations suggest that a rational cheater would likely attempt fewer cheating events than our analysis indicates, as the risks and uncertainties may outweigh the potential benefits.

This graph (see Figure 3) will change depending on the inspecting party's desired threshold of confidence in detecting cheating. The curve will shift upward if the inspecting party wishes to have at least e.g. 85% of detecting at least a single cheating attempt in a consecutive series of attempts. However, this is balanced against the cheating party's tolerance for the risk of getting caught. That tolerance will probably be much lower than 50%, and thus the curve and the "safe" number of cheating attempts will shift downward from the cheating party's perspective.

Y vs X for P = 0.5 and P = 0.85

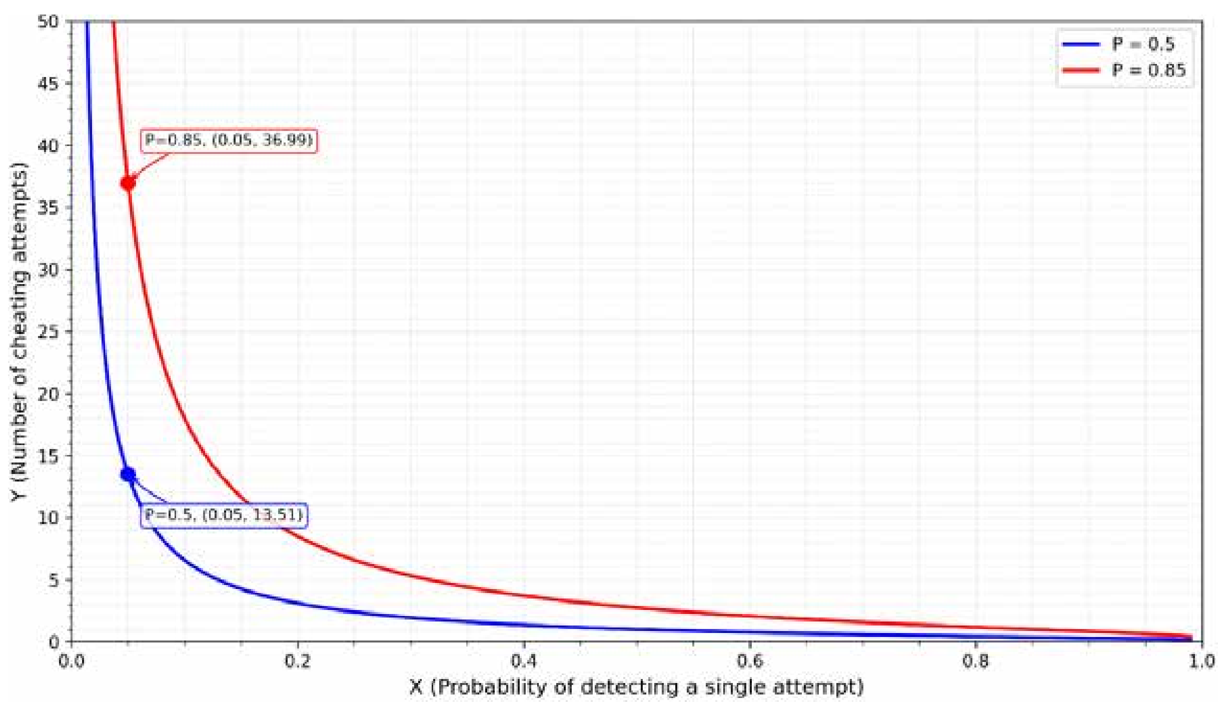

Figure 3: This graph illustrates how the number of cheating attempts (n) varies with the probability of detecting a single attempt (X) for two scenarios: when the overall probability of detection (P) is 50% (blue curve) and 85% (red curve). The points (0.05, 13.51) for P=0.5 and (0.05, 36.99) for P=0.85 are highlighted, demonstrating that a higher overall detection probability requires more cheating attempts for the same single-attempt detection probability. The curves show that as the probability of detecting a single attempt increases, fewer total attempts are needed to reach the specified overall detection probability.

About the Authors

Miles A. Pomper, the project leader, is senior fellow at the Washington, DC, office of the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies at Monterey. He has authored or co-authored several reports and book chapters on nonstrategic nuclear warheads, arms control, and deterrence in Europe, including Ensuring Deterrence Against Russia: The View from NATO States (2015). He is also the author or co-author of dozens of other reports and book chapters on nuclear arms control, nuclear nonproliferation, and nuclear and radiological terrorism. He is the former editor of Arms Control Today, the former lead foreign-policy reporter for the Capitol Hill publication CQ Weekly, and a former diplomat with the US Information Agency.

Rose Gottemoeller is the Steven C. Házy Lecturer at Stanford University's Freeman Spogli Institute for International Studies and its Center for International Security and Cooperation. Before joining Stanford, Gottemoeller was the deputy secretary general of NATO from 2016 to 2019, where she helped to drive forward NATO's adaptation to new security challenges in Europe and in the fight against terrorism. Prior to NATO, she served for nearly five years as US undersecretary of state for arms control and international security, advising the secretary of state on arms control, nonproliferation, and political-military affairs. While assistant secretary of state for arms control, verification, and compliance in 2009 and 2010, she was the chief US negotiator of the 2010 New Strategic Arms Reduction Treaty with Russia.

William M. Moon is a nonresident fellow at the Stimson Center. He was the global nuclear-security program manager for Cooperative Threat Reduction programs with Russia, China, Ukraine, Belarus, and Kazakhstan from 1992 to 2014. He led the implementation of more than $2 billion of nuclear-warhead-security programs in partnership with the Russian Ministry of Defense's 12th Main Directorate. He retired from the Defense Threat Reduction Agency in 2019.

Marshall L. Brown Jr. was the legal adviser to the US delegation during the negotiation of the Strategic Arms Reduction Treaty (START I), the Open Skies Treaty, the Comprehensive Nuclear-Test-Ban Treaty, the US-Poland missile-defense basing agreement, and the New Strategic Arms Reduction Treaty. He also participated in periodic implementation meetings for the Anti-Ballistic Missile Treaty, the Intermediate-Range Nuclear Forces (INF) Treaty, and START I, as well as in meetings on the Convention on Certain Conventional Weapons and in review conferences for the Biological and Toxin Weapons Convention and Chemical Weapons Convention. He served as attorney-adviser and assistant general counsel in the US Arms Control and Disarmament Agency, as force counsel in the Multinational Force and Observers (Sinai), and as attorney-adviser in the US State Department, from which he retired in 2010.

Ferenc Dalnoki-Veress is scientist-in-residence at CNS. A PhD physicist, he is focused on issues where science and policy meet, such as verification of nuclear-weapons agreements minimization of highly enriched uranium in civilian nuclear programs, spent-fuel management, emerging technologies, high-sensitivity particle detection, and neutrino physics.

Daniil Zhukov is a Program Coordinator at the Berkeley Risk and Security Lab, UC Berkeley. In this role, he manages BRSL's research, events, and wargaming portfolios. His research interests revolve around nuclear arms control and risk reduction, US and Russian nuclear policies, and crisis communications. He holds an MA in War Studies from King's College London and previously worked at Stanford University's Center for International Security and Cooperation as Rose Gottemoeller's staff research assistant.

Richard Gullickson has more than 45 years of experience in conducting research and managing projects in nuclear weapons effects, radiation measurements, directed energy weapons, and arms control technology. As an active-duty Air Force Officer and DoD civilian Gullickson worked at the Air Force Weapons Laboratory, the Lawrence Livermore National Laboratory, the Air Force Office of Scientific Research, the Defense Nuclear Agency, The Defense Advanced Research Projects Agency, The Strategic Defense Initiative Organization, and the Defense Threat Reduction Agency (DTRA). His final DTRA assignment was managing the Treating Verification Technologies Office. He holds a patent for detecting nuclear material on moving vehicles. As a DoD civilian he served as a member of the Senior Executive Service for more than 20 years.

Yanliang Pan is a Research Associate at the James Martin Center for Nonproliferation Studies and, in addition to his research activities, coordinates the Center's engagement with Chinese counterparts on issues related to nuclear nonproliferation and peaceful uses. His research has focused on the Russian and Chinese nuclear industries as well as on issues related to the nuclear fuel cycle and supply security. His ongoing research deals with the intersection between artificial intelligence and the nuclear agenda across safety, security, nonproliferation, research, and education. Yanliang holds a BSc/MA degree in Eurasian, Russian and East European Studies from Georgetown University and a MA degree in Nonproliferation and Terrorism Studies from the Middlebury Institute of International Studies at Monterey.

nonproliferation.org

Middlebury Institute *of*
International Studies at Monterey
James Martin Center for Nonproliferation Studies