2022 Data Authentication Demonstration: Exploration of Host and Inspector Confidence in Hardware, Software, and Data

Jay Brotz[4], Erin Connolly[4], Elin Enger[1], Martin Goliath[2], Neil Grant[3], Ian Hayes[3], Steinar Høibråten[1], Rob Hughes[3], Sindre Kaald[1], Justin Knowles[4], Peter Marleau[4], Sarah McOmish[3], Jeff Preston[4], Ole Reistad[1], Ben Stanley[3], Alicia Swift[4], Ryan Tan[4], Matthew Thornbury[4], Glen Warren[4], Jens Wirstam[2]

[1]*Norway* [2]*Sweden* [3]*United Kingdom* [4]*United States*

Abstract

The Quad Nuclear Verification Partnership (Quad) completed the Data Authentication Demonstration in June 2022 at Y-12 National Security Complex (Y-12). The Data Authentication Demonstration explored authentication (i.e., trust) and certification (i.e., safety and security) concepts on hardware, software, and data under representative constraints for a hypothetical nuclear disarmament scenario. The Quad consists of members from Norway, Sweden, the United Kingdom, and the United States. The Quad sought to demonstrate the use of equipment within sensitive facilities (such as Y-12), while exploring the impact of host-facility certification procedures on inspector authentication of the verification data produced. With this demonstration, the Quad investigated an approach to use inspector-provided technology in a host facility while also satisfying the host's certification needs. This demonstration used Sandia National Laboratories' wired Chain of Custody Item Monitor as the example technology, which was provided to Y-12 by a non-US Quad partner country. This paper will outline demonstration activities, outcomes, and findings with respect to host and inspector confidence.

1. INTRODUCTION

The Quad Nuclear Verification Partnership (Quad) consists of members from Norway, Sweden, the United Kingdom (U.K.), and the United States (U.S.), focused on multilateral approaches to nuclear disarmament verification. Within the partnership, the Quad researched equipment, procedures, data handling, and encryption necessary to maintain confidence in data generated during verification. The Quad held the Data Authentication Demonstration (DAD) to explore authentication and certification concepts developed by the Quad that pertained to hardware and data, using representative constraints for a hypothetical nuclear disarmament scenario. The DAD spanned four phases of work, culminating in a mock on-site inspection hosted at the Y-12 National Security Complex (Y-12) from June 13 to June 16, 2022.

During the DAD, the Quad sought to demonstrate the use of equipment within sensitive facilities (such as Y-12), while exploring the impact of host-facility certification procedures on inspector authentication of the verification data. With this demonstration, the Quad investigated an approach to use inspector-provided technology in a host facility, while also satisfying the host's certification needs. This demonstration used Sandia National Laboratories' (SNL's) wired Chain of Custody (CoC) Item Monitor (CoCIM) as the example technology [1].

1.1. Chain of Custody Item Monitor (CoCIM)

The CoCIM was the item of equipment chosen to be deployed into a sensitive area at Y-12 (Figure 1). It is an active seal that uses a fiber optic cable and a tamper-indicating enclosure to seal items. The CoCIM records every time that the fiber optic seal is opened and closed in the form of cryptographically signed messages, which can be retrieved when the CoCIM is attached to a laptop. The CoCIM uses public-private key cryptography to sign the open/close messages. The public-private key pair are generated during an initialization process, with the private key held on the CoCIM itself. The tamper-indicating enclosure is designed to ensure the private key is deleted if someone attempts to open the enclosure. The public key can be shared with anyone and allows the messages to be authenticated on any laptop.

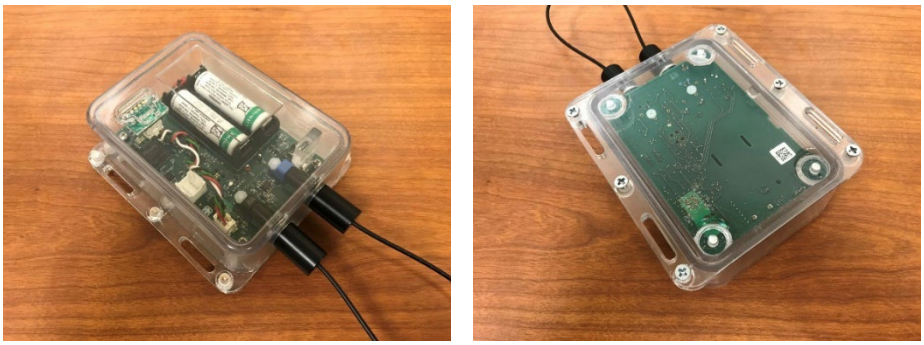

Figure 1. Front (left) and back (right) of closed CoCIM [1].

1.2. Demonstration Goals

The DAD built upon findings from the Quad LETTERPRESS exercise, hosted by the United Kingdom in 2017, but was not a full-scale exercise like LETTERPRESS. Instead, the DAD focused on the use of inspector-provided equipment in sensitive areas, and how initialization and authentication activities can help both the inspectors and hosts maintain confidence in the data generated. The demonstration had five goals:

- Goal 1: Investigate the possibility of using inspector-supplied equipment, with limited host inspection, for equipment that generates non-sensitive information, while maintaining confidence by all parties in the hardware and data.
- Goal 2: Investigate possible approaches for generating and transmitting data, while maintaining confidence by all parties in the data.
- Goal 3: Develop an understanding of how host safety and security concerns interplay with inspectors' confidence in the hardware and data generated.
- Goal 4: Develop an approach in which non-sensitive information is generated in a sensitive area in a manner in which all parties have confidence in the data.
- Goal 5: Provide exposure to all Quad members to a nuclear facility certification process and how that process may impact authentication of equipment and data.

1.3. Demonstration Scenario

The DAD consisted of four phases, which are described in Table 1, with a distinction between the elements of the DAD that were "in play" and those which had to happen "out of play" to facilitate the DAD. Phases 1 – 3 occurred before the in-person demonstration at Y-12 and tested host certification processes. Phase 4 consisted of a simulated routine on-site inspection of three CoCIMs under a hypothetical treaty, and took place over a three-day period at Y-12 in Oak Ridge, Tennessee. The scenario assumed that the Inspection Team would be familiar with the host facility. The representative host facility included a limited area that was hypothetically a warhead storage area; an Inspection Team work room that was not a limited area; and an x-ray vault for post-use inspection activities.

Table 1. Description of the four phases of the DAD

Phase	In Play	Out of Play
Phase 1: Host Certification	• A CoCIM copy[1], supporting equipment, and associated procedures were provided to Y-12 to allow certification of the CoCIM for deployment in the chosen location.	• The DAD plan document, the CoCIM copy and supporting equipment were

[1] The "CoCIM copy" was not used in the remaining three demonstration phases and was provided to Y-12 as an example unit to assist with equipment certification and demonstration approvals. Since the CoCIM copy was not to be used in the rest of the demonstration, it was possible for Y-12 to open the unit and even subject the unit to destructive analysis, if required.

Phase	In Play	Out of Play
	• Inspector laptops that were to be used in specified locations during Phase 4 for post-use inspection activities were authorized for use by Y-12.	provided to Y-12 for demonstration approvals. • DAD activities were approved by Y-12.
Phase 2: Inspector Initialization	• The Inspection Team (consisting of Quad members) produced two CoCIMs to initialize.[2] • CoCIM 1 was initialized during a virtual meeting in November 2021, with the Swedish participants undertaking the initialization with the other Inspection Team members participating virtually. • After initialization, CoCIM 1 was sent from Sweden to Y-12. • CoCIM 2 was initialized in-person at a later meeting in Sweden during May 2022. • Reference data for Phase 4 post-use inspections (e.g. photographs, serial numbers, and the public key) were generated and recorded during these initialization activities.	• SNL sent two CoCIMs and supporting equipment to Sweden, which would from hereon be treated as "Inspector-provided equipment."
Phase 3: Pre-visit Installation	• CoCIM 1 received at Y-12, and approved by the facility for use without needing to open the initialized CoCIM (relying upon data from Phase 1 to do so). • CoCIM 1 installed on a representative item container in a limited area. • Host collected data from CoCIM 1, after installation, reviewed it and then distributed the data to the Inspection Team. • Due to some technical difficulties, an additional CoCIM (CoCIM 3) was initialized by Y-12 and applied to the same container as CoCIM 1.	• Y-12 generated x-ray images and photographs of CoCIM 1 that were used in Phase 4 as data injects that were notionally created by the Inspection Team during initialization.
Phase 4: On-site Inspection	• Inspection Team arrived at Y-12 for 3 day mock on-site inspection, bringing CoCIM 2 with them. • Inspection Team installed CoCIM 2 on a second representative item container in a limited area. • Inspection Team visually inspected installation of CoCIMs 1 & 3. • Host retrieved data from all 3 CoCIMs and passed the data to Inspection Team. • All 3 CoCIMs removed and taken to unclassified lab space for post-use inspection to check integrity and identify any signs of tampering.	• Phase 4 ended with a hot wash session to discuss findings and after-actions. • Observers were present to record and evaluate all Phase 4 activities. • Post-event questionnaires were answered by all participants.

1.4. Demonstration Participants

The demonstration consisted of 7 Quad members, 5 observers / evaluators, and 8 Y-12 staff, totaling 20 participants (Figure 2). Some participants were U.S. citizens with clearances, but most were from other countries and did not hold U.S. clearances. Y-12 developed a security plan to manage visitor access, and also ensured that the number of participants met room size requirements, including for emergency egress.

[2] "Initialize" – the process by which the CoCIM is prepared for use. It involves recording images of the CoCIM for later comparison, checking the firmware, setting the frequency at which the CoCIM's state of health message is recorded, sealing the CoCIM case, and downloading the public key. These activities must occur before the CoCIM is deployed.

Figure 2. DAD Participants with a mock nuclear weapon

1.5. Out of Scope Elements

Except for the CoCIM, chain of custody (CoC) aspects during the DAD were notional. As examples of notional CoC, seals and tamper indicating enclosures were not to be used for inspector equipment (e.g., log books) during the DAD. The rationale for this decision was that CoC procedures and technologies were explored in great detail during LETTERPRESS, so the DAD aimed to build upon LETTERPRESS findings and explore new areas, particularly the authentication of hardware and data.

In order to limit exercise scope, authentication techniques were only explored for the CoCIM during the post-use inspection. The demonstration was also not focused on verifying declarations and notifications, other than at the minimum level required to evaluate inspector confidence that the CoCIMs had been applied properly, and that they were properly installed on the correct item (e.g., confirming that the CoCIM is applied to the correct item using the item's serial number). The DAD did not use radiological or nuclear items during the demonstration, since they are not necessary to test the DAD concepts.

In addition, the DAD took place in a representative facility from a security standpoint, but not fully from a safety standpoint. The demonstration was not occurring in a facility rated for explosives nor for nuclear explosives, but was for nuclear and radiological material, as well as for handling sensitive information. Certification of the CoCIMs for use, therefore, did not reflect the full safety requirements found in a nuclear explosives area, but did reflect the security requirements for operating in such an area.

2. OVERVIEW OF DAD PHASE 4 ON-SITE ACTIVITIES

2.1. Day 1: Tuesday, June 14, 2022

On Day 1, the DAD participants arrived at Y-12 to begin demonstration activities. First, the Inspection Team visually and tactilely confirmed proper installation of CoCIM 3, attached to a representative warhead container in a Limited Area, and that there were no signs of host tampering (Figure 3). The adhesive seals on the case exterior were also confirmed by the Inspection Team. Under observation of the Inspection Team, the host attached CoCIM 3 to a host laptop to collect data. The data was then provided to the Inspection Team via thumb drive.

Figure 3. Confirmation of CoCIM 3

Upon reading the CoCIM 3 data, it was noted that the time stamp was off by one hour. It was determined to be the result of the host laptop being in the wrong time zone (the laptop had not switched to daylight savings time).

During Phase 3 installation, the host discovered 2 instances of unsigned state of health messages in CoCIM 1 (which occurred in late November, while it was in the possession of the shipping company during transport from Sweden to Y-12, since it occurred several weeks after the initialization process in Sweden). The Inspection Team confirmed what the host had seen according to the activities outlined later in the next paragraph.

The same process was repeated for CoCIM 1 to confirm its integrity and to read out data using a host laptop. While conducting visual and tactile inspections of CoCIM 1, the Inspection Team noticed that when it was picked up, the internal red light flashed, indicating an opening/closing event was registered. This happened two times. Then, upon readout with the host laptop, the Inspection Team saw that CoCIM 1 was logging opening events that correlated to when the red light flashed. These events were logged in the CoCIM 1 data as an opening and a closing of the seal within the same second. The Inspection Team decided to replace the fiber optic cable, and used a specialized fiber optic cutting tool to cut the cable from the spool. When the fiber optic cable was changed, the issue was resolved. It was determined that using scissors to cut the original cable likely caused an uneven cable surface that then did not sit flush in the ferrule, leading to erroneous events being logged upon movement. Importantly, the Inspection Team were present with CoCIM 1 when the spurious open/close events occurred, meaning that there was no occasion on which the seal was logged as "open" whilst the Inspection Team was not present, except for the initial placement on the warhead container.

Afterwards, the Inspection Team installed CoCIM 2 on another treaty accountable item; the data was read out before and after installation using the host laptop. For unknown reasons, CoCIM 2 had a step-jump in the time stamps sometime between initialization in Sweden (which was correctly recorded in time) and deployment at Y-12, without any of the regular "State of Health" messages appearing to be missing. The step-jump was quite large at 9 hours. The step-jump occurred while CoCIM 2 was in Inspection Team possession, so did not appear to represent any tamper event.

Figure 4. Installation of CoCIM 2 by the Inspection Team

The participants broke for lunch, and the Inspection Team reviewed data generated thus far on Day 1. The Inspection Team then confirmed CoCIM 1 visually and tactilely, data was read-out by the host, CoCIM 1 was removed by the Inspection Team, and data was read-out by the host again. This process was repeated for the removal of CoCIM 3. The fiber optic loops were re-inserted in both CoCIMs to register a "close" event, and they were stored in the inspection area to await post-use inspection the following day. A summary of off-normal events for each CoCIM may be found in Table 2.

Table 2. Summary of CoCIMs and off-normal exercise events

CoCIM #	Initialization	Installation	Incorrect time stamp from host laptop read-out	Incorrect time stamp for unknown reason	Unsigned data events	Events logged upon moving CoCIM
1	Virtually by Inspectors (November 2021)	By Hosts (June 2022)	X		X	X
2	In-person by Inspectors (May 2022)	By Inspectors (June 2022)	X	X		
3	By Hosts (May 2022)	By Hosts (June 2022)	X			

2.2. Day 2: Wednesday, June 15, 2022

On Day 2, the Inspection Team removed CoCIM 2 using the same process outlined in the paragraph above. The Inspection Team, under observation of the Host Team, then conducted the post-use inspection procedures outlined in Reference [2] on all three CoCIMs. The post-use inspection procedures included visual inspection, tactile inspection, x-ray radiography (see Figure 5), firmware confirmation, hardware confirmation, software confirmation, and circuit board inspection. The adhesive seals on the case exterior were also confirmed by the Inspection Team. The participants broke for lunch, and then continued post-use inspection activities after lunch. In some cases, there was not enough time to take the data and then analyze it, so decisions had to be made to prioritize the evaluation of data collected; some data was notionally to be reviewed once the Inspection Team had returned to their home country. There were also discussions on the value of taking data and then analyzing it at home in the Inspection Team's country later. At the end of the day, Inspection Team equipment was cleared for release from the area by the facility's Radiation Control specialists.

Figure 5. X-ray Radiography during Post-use Inspection Activities

2.3. Day 3: Thursday, June 16, 2022

On Day 3, everyone completed a DAD Questionnaire to allow the Quad to determine how confidence changed compared to before the exercise. A hot wash was also held to discuss lessons learned, host and inspector confidence, and next steps.

2.3.1. Hot Wash Findings

Inspection Team:

- In general, it can be hard to evaluate confidence when the probability of potential host attacks are unknown.
- Can the Inspection Team have confidence in a CoCIM initialized by the Host Team in their absence?
    - The Inspection Team had no confidence before the inspection visit, but did gain more confidence in the data after data was readout periodically and seen to agree with the Inspection Team's data. However, because the Host Team opened and initialized the CoCIM, the private key is at risk. Different authentication procedures would be needed to gain confidence in the integrity of the private key in this scenario, and it may not even be possible.
    - In case of off-normal events, having a pool of spare Inspection Team-initialized CoCIMs at the host site (under joint CoC) would be valuable. However, as time goes on, the host has more time to tamper with the spares, so the value of this would decrease over time.
- Off-normal events
    - Time stamp issues in CoCIM 2 and CoCIM 3
        - CoCIM 2 had a 9-hour difference that was not a slow drift but a single jump in time
            - It was valuable to do another read-out of CoCIM 2 by the Inspection Team after initialization and immediately prior to shipping. This read-out provided documentation that the issue happened while in Inspection Team custody. Otherwise, this drift issue would have been discovered at the host location and could have led to false accusations.
        - CoCIM 3 had a 1-hour difference due to the host laptop being in the wrong time zone (Eastern Standard Time versus Eastern Daylight Time Savings Time)
            - It is important that the host laptop is properly updated before use.
        - In general, the timestamp issues made it difficult for both parties to determine if events were logged with the appropriate timestamp.
        - Having one watch or multiple synchronized clocks as the "trusted clock" that is set to universal time (UTC) would make inspections more efficient.

    - Logged events from movement of CoCIM 1[3]
        - It is important to properly cut and install the fiber optic cable
        - The negative impact was reduced since it happened in Inspector Team presence, but this would have had a dramatic impact if this had happened when Inspector Team was not present, and Host Team would have been surprised also because this may not have been seen (Host Team was not looking for this during installation)
- Overall Inspection Team confidence
    - The Inspection Team had the most confidence in CoCIM 2 because CoCIM 2 was hand-carried and installed by the Inspection Team, and the least confidence in CoCIM 3. Confidence in CoCIM 3 was particularly low because the authentication steps had not been designed to address a CoCIM initialized by the Host.

Host Team:

- Flexibility in the verification approach is important so that work can continue in unplanned or off-normal situations. During the DAD, there were changes or additions to DAD activities, chiefly due to off-normal events. By being able to assess that changes in activities were in agreement with the treaty scenario and inspector / host rights, inspection goals could be met.
- It was found that increased frequency of CoCIM read-outs was desirable because it enabled more opportunities to identify when something went wrong. At a minimum, read-outs immediately before and immediately after an installation or removal are recommended.
- For the DAD, the Inspection Team was physically allowed very near to the treaty accountable items, and was also allowed to install or remove CoCIMs. A host country may impose a stand-off distance from the treaty accountable item to ensure the safety of personnel and the item itself. In such a case, it may be reasonable for the host to remove the CoCIM and allow the inspector to visually / tactilely inspect the fiber optic cable post-removal, while remaining at an allowed stand-off distance from the item.
- Data management
    - Photographs needed to be reviewed by the host prior to release to the Inspection Team, but CoCIM data and x-ray image data did not.
    - Inspection team laptops did not need to be scanned because they did not enter the limited area, and laptops were approved by the host via paperwork that recorded laptop serial number, make, model, and use locations.
    - CoCIMs did not need to be scanned before entering the limited area because they were non-wireless.
    - For security reasons, thumb drives were controlled by the host, and data transfer could only be one way (from the host to the inspector) to prevent potential contamination of host computing resources. Thumb drives were tracked by the host by their serial number, and their use was recorded in a log.
- Overall Host Team confidence
    - In a true treaty scenario, after identifying errors with CoCIM 1, the Host Team likely would not have installed it (but did for the purposes of the exercise). This is because a non-functioning CoCIM could falsely indicate noncompliant behavior.
    - The Host Team had more confidence in CoCIM 2 than in CoCIM 1 since the timestamp problem was less worrisome than unsigned data from their perspective.

[3] The Quad did a comparison between in-cabin luggage (CoCIM 2) and under-plane hold luggage (CoCIM 1 & "CoCIM Norway" & "CoCIM UK") to see if that was the initial cause of the CoCIM 1 issues (unsigned data). In-cabin luggage had no issues, and neither did CoCIM Norway and CoCIM UK. May need to explore impact of shipping / very cold temperatures in a cargo hold on the unsigned data issue.

- The Host Team had the most confidence in CoCIM 3 since the Host Team had initialized and installed it.

Evaluation Team:

- Overall, the evaluation team thought the DAD successfully met its goals because the Quad was:
  - Able to demonstrate the release of non-sensitive data from a sensitive location, and also the ability to do this repeatedly and on realistic timescales
  - Able to demonstrate authentication
  - Able to provide nuclear facility experience to the Quad so everyone may understand the certification process better
  - Able to show that the CoCIM could leave with the Inspection Team at the end of the inspection, with the release process completely transparent (with no "black box" processes while in host custody)
  - The evaluation team recommended potential areas for future work:
    - Explore how to sign data
    - It would be valuable to continue to increase the level of scrutiny in Quad demonstrations and make things more challenging to see how that may impact confidence
    - It would be beneficial to study off-normal events – CoCIM malfunctions, fire alarms, etc. – and how to resume work and maintain confidence in such a situation

2.3.2. DAD Questionnaire

A questionnaire was completed by DAD participants and Y-12 host staff at key points in the DAD planning and execution process to assess how the following changed over time: (a) general confidence and trust; (b) CoCIM-specific confidence and trust; (c) Inspector/Host confidence and trust; and (d) factors contributing to confidence and trust. The questionnaire was designed to provide evidence in support of the DAD goals, and to assess how and if the CoCIM use, deployment, and authentication procedures could contribute to confidence in the data it provides.

For all three CoCIMs, both groups found their confidence in the correct functionality to be at least "I believe the statement is probably true". On average, everybody rated the consistency of CoCIM 1 and CoCIM 2 with the certified unit to be at least "I believe the statement to be true", and only CoCIM 3 garnered a slightly lower rating ("most likely true") from the Inspectors, most probably because they had never had CoCIM 3 in their possession before it was installed. All participants largely believed that a CoCIM, and the data it generated, prevented unmonitored access to the secured items.

Qualitatively, the Inspectors appear to have gained confidence after carrying out the authentication procedures during the DAD, whilst the Hosts largely appear to have slightly reduced confidence after the authentication stage. However, the only Host score that dipped below being "probably true" was for whether CoCIM 1 and CoCIM 2 were "recording the intended data", and these were the two CoCIMs which were Inspector-initialized and displayed "off-normal behavior" in terms of unexplained timestamp drifts or events being logged inappropriately. All participants believed it to be true that CoCIM 3 was recording the intended data, and *only* the intended data, with the Inspectors also confident in CoCIM 1 and CoCIM 2.

Both the Inspectors and the Hosts scored the "in-person" data transfer as providing more confidence than the two remote methods which involved emailing the data. This doesn't necessarily reflect the method of transfer but might indicate a residual lack of confidence in data that is retrieved without Inspectors being physically present. It illustrates that the inclusion of cryptographic digital signatures on the data does not fully compensate for the Inspectors' perceived drop in confidence from not being present during data retrieval.

Unfortunately, it was not possible to separate out whether receiving the data remotely beforehand helped to maintain confidence, as there were no questionnaire results from Phase 3 (after data transmission but before Inspectors arrive in person).

In all, the participants believed it is *at least* "probably true" that each other behaved appropriately and did not cheat during the DAD. Interestingly, both groups provide almost the same score for belief that the CoCIM has not been tampered with, once the authentication procedures have been completed.

When considering the factors that contribute to confidence in the CoCIM and the data it generates, it is evident that the initialization process is of utmost importance to the Inspectors. Confidence in the data from the CoCIM appears to be drawn from two major considerations – knowing the CoCIM was correctly installed, and verifying that the data is digitally signed. Verifying the installation can be done at a later date via in-person inspection, but verifying that the data produced by the CoCIM is correctly signed can only be done if one controls, or has confidence in, the initialization process.

3. CONCLUSIONS

The DAD successfully met all five goals, with the performance evaluation against each goal outlined below:

- Goal 1: Investigate the possibility of using inspector-supplied equipment, with limited host inspection, for equipment that generates non-sensitive information, while maintaining confidence by all parties in the hardware and data.
    - The DAD was able to meet this goal, and showed that the use of inspector-supplied equipment, with limited host inspection, is more than a possibility – it can be a reality.
- Goal 2: Investigate possible approaches for generating and transmitting data, while maintaining confidence by all parties in the data.
    - The DAD was able to meet this goal, and demonstrated that data could be transmitted multiple ways: by host email, host thumb drive, connection of a CoCIM to a host laptop, and connection of a CoCIM to an inspector's laptop.
- Goal 3: Develop an understanding of how host safety and security concerns interplay with inspectors' confidence in the hardware and data generated.
    - The DAD was able to meet this goal, and the participants learned a lot regarding host safety and security concerns, even though there were some differences between the certification for a limited area versus a material access area. There is also a better understanding of how a host might escort an Inspection Team and provide access to the host site.
- Goal 4: Develop an approach in which non-sensitive information is generated in a sensitive area in a manner in which all parties have confidence in the data.
    - The DAD was able to meet this goal, although off-normal events did reduce overall confidence. However, each CoCIM provided unique opportunities to explore how various approaches and off-normal events can impact confidence.
- Goal 5: Provide exposure to all Quad members to a nuclear facility certification process and how that process may impact authentication of equipment and data.
    - The DAD was able to meet this goal by providing exposure to all Quad members to a nuclear facility certification process.

REFERENCES

[1] S. Hammon, S. Schwartz, J. R. Wade, R. Helguero and T. Hunt, "Wired Chain of Custody Item Monitor (CoCIM) User Manual v5 (SAND2020-13933 O)," Sandia National Laboratories, 2020.

[2] S. Hammon, "Wired Chain of Custody Item Monitor (CoCIM) Inspection Procedures (SAND2021-11427 O)," Sandia National Laboratories, 2022.

[3] A. Swift, "Data Authentication Demonstration Plan," Y-12 National Security Complex, 2022.

[4] Quad Verification Technologies Workstream, "Data Authentication Demonstration: Questionnaire and Analysis," 2022.

Acknowledgements: *Development of this paper was funded by the U.S. National Nuclear Security Administration's Office of Nuclear Verification (NA-243).*