IT Security
Supply Chain
OT Security
Insider Threat
Physical Security
Interoperable Communications

CISA Insights

DEFEND TODAY,
SECURE TOMORROW

CHAIN OF CUSTODY AND CRITICAL INFRASTRUCTURE SYSTEMS

Chain of custody is a complex process. Often associated with the preservation of evidence for law enforcement, chain of custody also plays an important role in security and risk mitigation for critical infrastructure sectors and their assets. Without secure chain of custody practices, critical infrastructure systems and assets could be unknowingly accessed and manipulated by threat actors. The integrity of critical infrastructure assets and systems could also be questioned, with the inability of critical infrastructure owners and operators to prove otherwise.

This CISA Insights provides an overview of what chain of custody is, highlights the potential impacts and risks resulting from a broken chain of custody, and offers critical infrastructure owners and operators an initial framework for securing chain of custody for their physical and digital assets.

WHAT IS CHAIN OF CUSTODY?

Chain of custody is a process used to track the movement and control of an asset through its lifecycle by documenting each person and organization who handles an asset, the date/time it was collected or transferred, and the purpose of the transfer. Examples of assets include equipment, infrastructure, evidence, systems, and data. Maintaining the chain of custody increases transparency and enables accountability for actions taken on the asset. In practice, chain-of-custody documentation can support risk mitigation by reducing the opportunity for malicious actors to tamper with the asset (e.g., equipment, data, or evidence).

Examples of Physical Chain of Custody

- **Chemical Sector:** Freight railroad carriers and rail hazardous materials shippers and receivers must implement chain-of-custody requirements to ensure a positive and secure exchange of hazardous materials.
- **Election Infrastructure Subsector**: Chain-of-custody practices for an election include control forms, tamper-evident seals, and serialized equipment to provie assurances that ballots are authentic and accounted for throughout the election.

Examples of Digital Chain of Custody

- **Healthcare and Public Health Sector:** Chain-of-custody processes at U.S. Department of Health and Human Services-certified laboratories ensure that no unauthorized personnel handle specimens or gain access to the laboratory processes or areas where records are stored.
- **Financial Services Sector:** Financial institutions must comply with chain-of-custody regulations on the transfer of electronic data between institutions or into storage to prevent loss of data or interference.

BROKEN CHAIN OF CUSTODY

A break in the chain of custody refers to a period during which control of an asset (e.g., systems, data, or infrastructure) is uncertain and during which actions taken on the asset are unaccounted for or unconfirmed. Such breaks present opportunities for malicious activity that may compromise the integrity of the asset. In the event that the chain of custody is broken, the integrity and reliability of the asset's system, components, and accompanying data should be evaluated as to whether they can be restored to their original state and reinstated into the asset.

A break in the chain of custody occurring due to a non-validated organization or bad actor gaining custody or access increases the risk that the integrity or reliability of the asset cannot be restored. The available information may not be sufficient to prove that the confidentiality, integrity, or availability of the asset was not compromised.

Potential Impacts of a Broken Chain of Custody

- The integrity of the system and its underlying data can no longer be trusted.
- The reliability, accuracy, and security of records in question – physical or digital – cannot be guaranteed.
- The systems and data may be rendered inadmissible in a court of law.
- The inability to provide evidence that a system has not been compromised results in the inability to determine if a malicious actor (or any actor for that matter) has gained access to and/or manipulated the systems and data.

FRAMEWORK FOR SECURING CHAIN OF CUSTODY

To address risk and improve security and resilience, owners and operators of critical infrastructure can utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to establish chain-of-custody standards, guidelines, and practices. NIST created the CSF—which is a flexible, repeatable, performance-based, and cost-effective model that consists of five concurrent and continuous functions—to improve risk management in critical infrastructure. See the lists below for actionable steps for each CSF function.

Identify

Develop an organizational understanding to manage physical and cybersecurity risk to systems, people, assets, data, and capabilities.

- Identify critical assets within the organization.[1]
- Inventory all systems, devices, software, data, and people.
- Catalog external systems, especially dependent systems and/or processes that the organizations critical assets may integrate with, especially if those systems or processes are outside the control of the organization.
- Document the digital and analog forms or logs that track transactions and access.
- Routinely assess the logs and forms to understand if there are any gaps in transactions or access that could lead to a break in chain of custody.
- Evaluate your preservation rules to determine if they meet the organization's business needs.

Protect

Develop and implement a chain of custody plan and appropriate safeguards to ensure critical services, systems, and data are properly secured while at rest and in transit. Protective measures keep unauthorized and malicious actors out.

- Implement access control, both physically and electronically, to assets and facilities.
- Ensure that individuals are only authorized to access systems, data, and facilities that are pertinent to their job functions—use the Principle of Least Privilege.
- Ensure network integrity is protected and remote access is managed.
- Implement continuous monitoring of transactions, activities and access control processes.
- Manage information and records consistent with the organization's risk strategy to protect confidentiality, integrity, and availability of information.

Detect

Develop and implement appropriate activities to identify the occurrence of a chain-of-custody breach. Detective measures provide evidence that a breach has occurred.

[1] Pursuant to Executive Order (EO) 14028 on Improving the Nation's Cybersecurity, issued on May 12, 2021, the National Institute of Standards and Technology (NIST) published a definition of the term 'critical software'. Available: https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf

- Log all transactions electronically (ex. Audit or event logs) or physically through chain of custody documents.
- Track each asset independently by uniquely identifying each asset, such as tamper-evidence or serialization.
- Establish incident alert thresholds.
- Guarantee continuous monitoring and/or alerting of detective measures. If the chain of custody breaks without having established monitoring measures, an incident can go undetected.

Respond

Develop appropriate activities to implement in response to a detected breach of the chain of custody. Response measures allow the organization to determine the impact and consequences of the breach.

- Establish processes to receive, analyze, and respond to a breach, loss of integrity, or preservation to the chain of custody records.
- Investigate notifications from detection systems.
- Determine if the impact of breach leads to a reportable incident.
- Report incidents consistent with established criteria.
- Ensure personnel know their roles and order of operations when a response is required.
- Provide strict oversight of forensic activities being performed, including validating personnel, to ensure the chain of custody and integrity of the systems, data, and any evidence collected.

Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any critical services, systems, or data that were impaired due to the chain-of-custody breach or cybersecurity incident.

- Execute recovery processes and procedures to ensure the restoration of systems or assets affected by the incident.
- Sanitize media in accordance with NIST Special Publication 800-88 Revision 1.
- Review and assess hardware to determine whether system components have been replaced or modified in any way.
- Restore systems using a validated version of the firmware and software (e.g., trusted build).
- In cases where critical infrastructure systems are required to undergo certification, the accredited certifying body may need to review the affected systems for recertification.
- If systems or data must be turned over to a validated entity, processes should be in place for reassuming and validating the chain of custody prior to reintegrating those systems or data into your infrastructure. These processes should potentially include media sanitization, trusted build installation, system recertification, acceptance testing protocols, etc.
- There may be situations where it is not possible to re-establish the chain of custody or integrity of the systems or data (i.e., loss of the chain of custody). In those instances, consider decommissioning and replacing assets of concern. There may be situations where the time, cost, and/or expertise to recover, re-establish the chain of custody, and potentially recertify systems is not practical. A recovery plan should include procedures for how to handle such a scenario, including the complete replacement of the assets.

AUDIT YOUR PROCESSES

Critical infrastructure owners and operators should routinely audit chain of custody processes to prove that the authenticity of the data collected has been maintained across all stages. Audits should look for evidence that demonstrates the effectiveness and durability of the procedures, processes, systems, and training. Trialing chain of custody processes also provides owners and operators the opportunity to ensure there are no gaps in the chain of custody process, and that sufficient evidence exists to maintain a defensible trail of collected data for a litigation or investigation.

RESOURCES

Definition of Critical Software Under Executive Order (EO) 14028: https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf

International Organization for Standardization, ISO 22095:2020 Chain of Custody – General Terminology and Models: https://www.iso.org/standard/72532.html?browse=tc

National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology, Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

National Institute of Standards and Technology Special Publication 800-88 Revision 1, Guidelines for Media Sanitization: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf