CRITICAL INFRASTRUCTURE CONTROL SYSTEMS CYBERSECURITY PERFORMANCE GOALS AND OBJECTIVES

As of 9/21/2021

On Wednesday, July 28, 2021, the President signed a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. The National Security Memorandum establishes a voluntary initiative intended to drive collaboration between the Federal Government and the critical infrastructure community to improve cybersecurity of control systems. It instructs the Department of Homeland Security (DHS) to lead the development of preliminary cross-sector control system cybersecurity performance goals as well as sector-specific performance goals within one year of the date of the National Security Memorandum. These goals are intended to provide a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.

To inform the development of the cross-sector performance goals, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) conducted an initial crosswalk of available control system resources and recommended practices that were produced by the government and the private sector. The crosswalk focused on the following documents:

- CISA Cyber Essentials (https://www.cisa.gov/cyber-essentials)
- CISA Cybersecurity Best Practices for Industrial Control Systems (https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems)
- CISA Pipeline Cyber Risk Mitigation Infographic (https://www.cisa.gov/publication/pci-cyber-risk-infographic)
- CISA Recommended Practice: Defense in Depth (https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_CONTROL SYSTEM-CERT_Defense_in_Depth_2016_S508C.pdf)
- Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards Guidance (https://www.cisa.gov/publication/cfats-rbps-guidance)

- NRC Draft Regulatory Guidance (DG)-5061, “Cyber Security Programs for Nuclear Power (https://www.nrc.gov/docs/ML1801/ML18016A129.pdf)
- NIST SP 800-82, Rev 2, “Guide to Industrial Control Systems (ICS) Security.” (https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final)
- NISTIR 8183, Rev 1, “Cybersecurity Framework Version 1.1 Manufacturing Profile.” (https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final)

After reviewing the documents listed above, CISA and NIST identified nine categories of recommended cybersecurity practices and used these categories as the foundation for preliminary control system cybersecurity performance goals. Each of the nine goals includes specific objectives that support the deployment and operation of secure control systems that are further organized into baseline and enhanced objectives.

Baseline objectives represent recommended practices for all control system operators while the enhanced objectives include practices for critical infrastructure supporting national defense; critical lifeline sectors (i.e. energy, communications, transportation, and water); or where failure of control systems could have impacts to safety. DHS will coordinate with its interagency and private sector partners to determine the applicability of the enhanced objectives within each sector. In addition to the objectives, Example Evidence of Implementation is provided for each objective to demonstrate what successful implementation of an objective might entail for an organization. Successfully implementing all baseline objectives would equate to successful implementation of a goal.

It is important to note that while all of the goals outlined in this document are foundational activities for effective risk management, they represent high-level cybersecurity best practices. Implementation of the goals and objectives listed here is not an exhaustive guide to all facets of an effective cybersecurity program. These preliminary goals and objectives were developed and refined with as much interagency and industry input as practical for the initial timeline using existing coordinating bodies. DHS expects to conduct much more extensive stakeholder engagement as the goals are finalized in the coming months.

Preliminary Performance Goals and Specific Objectives

The following section outlines the preliminary goals and objectives described in the preceding section. The order of the goals and objectives is not intended to imply a prioritization or specific progression of operations.

Collapse All Sections

Risk Management and Cybersecurity Governance

GOAL: Identify and document cybersecurity risks to control systems using established recommended practices (e.g., NIST Cybersecurity Framework, NIST Risk Management Framework, International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443, NIST Special Publication (SP) 800-53, NIST SP 800-30, NIST SP 800-82) and provide dec resources to address cybersecurity risk and resiliency through planning, policies, funding, and trained personnel.

RATIONALE: A formal risk management process provides standard terminology, documents risks, identifies roles and responsibilities, and is used by management to understand and manage risks, estimate impacts, and define responses to incidents.

Baseline Objectives

- Identify, document, and prioritize known risks to control systems
    - **Sample Evidence of Implementation:** *Organization has completed and documented a risk register and risk assessment using an established recommended practice on all control systems; the organization has a plan for updating them on a regular (e.g., annual, semi-annual) basis*
- Establish and enforce policies that accept, avoid, mitigate, or transfer identified high-priority risks including outlining acceptable use of, and access to, control system assets
    - **Sample Evidence of Implementation:** *Organization has provided documented policies (e.g., procedures, processes, plans, standard operating procedures) that address high-priority risks and has an established governance structure for updating and communicating that guidance*
- Demonstrate effective management support for cybersecurity programs
    - **Sample Evidence of Implementation:** *Organization has a named Chief Information Security Officer, or someone filling a similar role, with clearly defined authorities and dedicated resources*
- Provide regular dedicated funding sufficient to perform the objectives identified in these performance goals and any other sector or corporate cybersecurity requirements, including the cost of qualified personnel.
    - **Sample Evidence of Implementation:** *Organization has consistent funding for cybersecurity initiatives within the annual budget that allows for long-term planning and investment*

Architecture and Design

GOAL: Integrate cybersecurity and resilience into system architecture and design in accordance with established recommended practices for segmentation, zoning, and isolating critical systems (e.g., Industrial Control Systems-Computer Emergency Response Team Defense in Depth guide, Purdue Diagram) and review and update annually to include, as appropriate, any lessons learned from operating experience consistent with industry and federal recommendations.

RATIONALE: Integrating cybersecurity and resilience into system architecture and design is intended to prevent, detect or delay, respond to, and mitigate the consequences of malicious acts or other acts that could compromise cybersecurity. Properly segmenting a network provides increased access control, making it easier to restrict and monitor user access to systems. Network segmentation and segregation, with air gaps and properly implemented Access Control Lists (ACL), can help limit the scope of an incident and can also improve network performance because broadcast domain traffic can be minimized.

Baseline Objectives

- Ensure that cybersecurity is considered when new control systems are designed, develo and updated
    - **Sample Evidence of Implementation:** *Organization applies a clearly defined process for identifying and addressing potential impacts to control system cybersecurity before any new hardware or software is installed into the control system environment*
- Identify and document an inventory of software, hardware, and other systems with administrative access to prioritize activities such as continuous monitoring efforts and vulnerability management.
    - **Sample Evidence of Implementation:** *Organization maintains a constantly updated inventory of systems with administrative access*
- Protect the boundary of the control system
    - **Sample Evidence of Implementation:** *Organization employs firewalls, access control lists, and one-way communication diodes to protect the boundary of the control system*
- Ensure physical segmentation for control systems in adherence with established standards or recommended practices (e.g., NIST SP 800-53, NIST SP 800-82,ISA/IEC 62443), to include wireless configuration, hardware, and software controls that limit the ability to access or modify control system assets to individuals with a demonstrated need for access on established guidelines. Document, manage, and mitigate vulnerabilities discovered in the control systems
    - **Sample Evidence of Implementation:** *Organization completes a regular (e.g., semi-annual) system architecture review that includes a documented improvement plan for addressing vulnerabilities that pose a risk to control systems*

Enhanced Objectives

- Implement, integrate, and validate a Zero-Trust architecture
    - **Sample Evidence of Implementation:** *Organization completes a regular (e.g., semi-annual) Zero-Trust architecture review that includes a documented improvement plan for addressing any significant vulnerabilities or findings*

Configuration and Change Management

GOAL: Document and control hardware and software inventory, system settings, configurations, and network traffic flows throughout control system hardware and software lifecycles.

RATIONALE: Configuration and change management ensures that the organization's cybersecurity program objectives remain satisfied by ensuring that new systems are deployed in a secure consistent state and maintain this state as changes are made throughout their lifecycles. It reduces the risk of outages due to configuration issues and security incidents through improved visibility and tracking changes to the system.

Baseline Objectives

- Employ documented change management rules and procedures to ensure that an inventory of all control system firmware, software, and hardware with baseline configurations is recorded and maintained and that changes to configurations or systems are properly reviewed and recorded
    - **Sample Evidence of Implementation:** *Organization has written policies that are enforced requiring control systems to be inventoried, baseline equipment configurations to be recorded, and all*

changes logged

- Ensure that factory settings for all new firmware, software, and hardware are reviewed and updated to remove unnecessary permissions, services and/or programs
  - **Sample Evidence of Implementation:** *Organization has checklists, standard operating procedures, or other documented policies for reviewing firmware, hardware, and software capabilities against the demonstrated needs of the system to ensure that unnecessary services (e.g., ports) are disabled prior to installation*
- Limit the ability to change control system configurations to approved personnel with a demonstrated need for access (least privilege)
  - **Sample Evidence of Implementation:** *Organization requires elevated permissions for access to control systems, requires written justification from a manager for all staff requesting access, and reviews access on a semi-annual basis to ensure that only staff with a need-to-know have access to sensitive systems*
  - **Sample Evidence of Implementation:** *Organization requires separate elevated accounts for control systems; these accounts should not, unless needed or required, be tied to traditional IT. Additionally, daily work that does not require permission elevation should be completed by an account with least privilege*

Enhanced Objectives

- Conduct network baseline analysis on control systems and networks to understand approved communication flows
  - **Sample Evidence of Implementation:** *Organization monitors network traffic against a recorded baseline and can identify, investigate, and isolate (if appropriate) anomalous traffic to minimize impacts to the delivery of services to customers*

Physical Security

GOAL: Physical access to systems, facilities, equipment, and other infrastructure assets, including new or replacement resources in transit, is limited to authorized users and are secured against risks associated with the physical environment.

RATIONALE: Limiting physical access to only authorized individuals protects against malicious actors gaining physical access to control system components. These protections also help prevent unintentional damage.

Baseline Objectives

- Restrict physical access to control systems and connected equipment to authorized personnel with a need for access
  - **Sample Evidence of Implementation:** *Organization secures all human machine interfaces, terminals, and other control system hardware behind locked doors and maintains access logs to track personnel entering and exiting the secured space*
  - **Sample Evidence of Implementation:** *Organization has an established process for determining and documenting access requirements (e.g., specific requirements defining “need for access”) and implements a process of granting the access, periodically reviewing the access, and revoking access when no longer required*

- Ensure that unauthorized portable media devices and other hardware are unable to be c control systems
  - **Sample Evidence of Implementation:** *Organization has procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices*
- Establish environmental controls to maintain temperature and other physical factors that can damage sensitive equipment
  - **Sample Evidence of Implementation:** *Organization maintains a failover system that provides backup power to environmental controls for server rooms and other sensitive equipment in the event of an electrical outage*

Enhanced Objectives

None

System and Data Integrity, Availability, and Confidentiality

GOAL: Protect the control system and its data against corruption, compromise, or loss.

RATIONALE: Protecting the control system and its data against corruption, compromise, or loss is vital to its operation.

Baseline Objectives

- Limit logical access to control systems to individuals with a demonstrated need-to-know
  - **Sample Evidence of Implementation:** *Organization implements a role-based permission scheme for all accounts and ensures that account managers are informed of changes to users' statuses and needs*
- Prevent unauthorized use of control systems by changing default passwords, using strong password policies and access logs where feasible.
  - **Sample Evidence of Implementation:** *Organization establishes exclusive user account and password policies for control systems requiring multifactor authentication, account lockout procedures, and unique trust stores in control system environments*
- Prevent unauthorized access from remote users
  - **Sample Evidence of Implementation:** *Organization has a written policy that prohibits persistent remote access, catalogues and monitors all remote connections to the network, and investigates and validates every communication to a new IP address or domain from the control system environment*
- Ensure that data in transit is protected against unauthorized access or manipulation
  - **Sample Evidence of Implementation:** *Organization requires that all control system data transmissions employ end-to-end encryption using transport layer security (TLS) to protect the data in transit; legacy equipment that is unable to leverage encryption is prioritized for upgrade or replacement*
- Ensure that data at rest is protected against unauthorized access or manipulation
  - **Sample Evidence of Implementation:** *Organization requires that all hard drives storing sensitive control system data employ encryption and data loss prevention solutions that block or limit the connection of USBs, mobile devices, and removable storage drives; legacy equipment that is unable to leverage encryption is prioritized for upgrade or replacement*

Enhanced Objectives

- Limit and control the flow of data between the IT and control systems
  - **Sample Evidence of Implementation:** *Organization employs firewalls, access control lists, and one-way communication diodes to control the flow of data to and from the control systems*
- Allow only approved and tested changes to be applied to control systems
  - **Sample Evidence of Implementation:** *Organization monitors for unauthorized hardware, software, and configuration changes on control systems and has an established process for documenting and reporting unauthorized changes to control systems managers*
- Build crypto agility into control system design to enable rapid implementation of new cryptographic primitives and algorithms
  - **Sample Evidence of Implementation:** *Initial configuration parameters in newly acquired systems are set to enable future changes to encryption algorithms*
- Implement multifactor authentication for remote access
  - **Sample Evidence of Implementation:** *Organization requires multifactor authentication for remote access to the control system*

Continuous Monitoring and Vulnerability Management

GOAL: Implement and perform continuous monitoring of control systems cybersecurity threats and vulnerabilities.

RATIONALE: Continuous monitoring ensures that the periodic review and testing of security controls, processes, and procedures are conducted to confirm that the established security controls remain in place and that change in the system, network, environment, or emerging threats does not diminish the effectiveness of these controls, processes, or procedures. Vulnerability management ensures that the technical and operational elements are sufficiently protected against adversaries' attack methods, which often include targeting outdated and unpatched systems.

Baseline Objectives

- Organization employs a logical schedule to complete continuous monitoring, vulnerability assessments, and penetration testing.
  - **Sample Evidence of Implementation:** *Organization conducts regular table-top exercises, penetration testing, and vulnerability evaluations of internal and external systems*
- Implement anti-virus and anti-malware file integrity checking and anti-phishing technologies where feasible to prevent, deter, detect, and mitigate malware
  - **Sample Evidence of Implementation:** *Organization uses antivirus and antimalware software to scan for malware and protect systems from potential threats*
- Manage cybersecurity vulnerabilities by installing patches to correct known issues. Prioritize patching of personal computing machines used in human-machine interfaces, database servers, and engineering workstations
  - **Sample Evidence of Implementation:** *Organization has a policy for tracking control system common vulnerability enumerations (CVEs)Common Vulnerabilities and Exposures that affect their systems and apply patches (after testing) when available and perform risk analysis and risk mitigation when a patch is not forthcoming by a vendor.*

- Monitor control systems for malicious activity on control systems
  - **Sample Evidence of Implementation:** *Organization monitors for and reports suspicious behavior including simultaneous logins, TOR traffic, outside the office logins, and logins occurring outside normal business hours and employs an intrusion detection system to create alarms for control system network traffic outside normal operations*

Enhanced Objectives

- Align protection systems to known threat and vulnerability
  - **Example metric:** *Organization implements all applicable protections from public and industry threat and vulnerability advisories and alerts*
- Employ application control
  - **Sample Evidence of Implementation:** *Organization employs application control to prevent unauthorized software applications and executable files from executing*

Training and Awareness

GOAL: Train personnel to have the fundamental knowledge and skills necessary to recognize control system cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.

RATIONALE: Comprehensive cybersecurity awareness training is one of the best ways to help protect against and mitigate cyber-attacks and prevent possible breaches.

Baseline Objectives

- Ensure that control system operators and administrators understand cybersecurity concepts, terminology, activities, and the threat environment associated with implementing cybersecurity recommended practices
  - **Sample Evidence of Implementation:** *Organization requires regular (e.g. semi-annual or annual) cybersecurity awareness training provided to all employees and role-based training to control system operators and administrators*
- Ensure control system operators and cybersecurity personnel recognize the indicators of potential compromise and what steps they should take to ensure that a cybersecurity investigation succeeds
  - **Sample Evidence of Implementation:** *Organization has dedicated resources and funding available for control system operators to attend technical trainings and conferences on latest indicators of potential compromise and best practices for response*

Enhanced Objectives

- Ensure control system operators and cybersecurity personnel receive training in control systems security at the intermediate and advanced levels.
  - **Sample Evidence of Implementation:** *Organization provides either web-based or instructor-led training on control systems security to ensure an overall understanding of their roles and responsibilities*
  - **Sample Evidence of Implementation:** *Table-Top Exercise (TTX) Aligns with the five steps of the cybersecurity lifecycle. Operators conduct TTXs to identify, protect, defend respond and recover. The goal is to become proactive and not reactive to incidents*

- **Sample Evidence of Implementation:** *Operators participate in control systems and o technologies working groups and attend conferences*

Incident Response and Recovery

GOAL: Implement and test control system response and recovery plans with clearly defined roles and responsibilities.

RATIONALE: Dedicated resources and established plans limit impacts of a cyber-attack and minimize the time to reconstitute critical systems and functions.

Baseline Objectives

- Develop control system cybersecurity response and recovery plans
  - **Sample Evidence of Implementation:** *Organization maintains written (digital and physical) control system cybersecurity response plans that include scenario specific annexes outlining the roles and responsibilities of all employees involved in emergency response activities; plans are updated regularly (e.g., every three years)*
- Ensure that control system functions are prioritized and reconstituted according to their impact to operations
  - **Sample Evidence of Implementation:** *Organization conducts a regular (annual or bi-annual) business impact assessment to prioritize resources and identify which systems must be recovered first*
- Establish contingency plans to maintain the delivery of critical services in the event of a control system outage
  - **Sample Evidence of Implementation:** *Organization maintains and regularly (annual, bi-annual, or after an incident) updates contingency plan in the event of a control system outage*
- Implement cybersecurity response plan when an event occurs
  - **Sample Evidence of Implementation:** *Organization has an established process for reporting incidents internal chain of command (e.g., shift leaders or managers) and appropriate authorities including local law enforcement, Cybersecurity Infrastructure Security Agency, Federal Bureau of Investigation, and other federal agencies within 12 hours of discovery (including events based on government-provided indicators of compromise)*
  - **Sample Evidence of Implementation:** *Organization detects the event, escalates the event as needed, declares a cybersecurity incident, and implements response activities, as documented in the cybersecurity incident response plan*
- Ensure the ability to reconstitute systems following an incident with minimal disruption to services
  - **Sample Evidence of Implementation:** *Organization policies require that physical backups for all critical system files be maintained, updated, and tested regularly (e.g., quarterly) and that offline copies are protected using encryption and stored in a locked safe*

Enhanced Objectives

- Develop support structures to enable more effective incident response
  - **Sample Evidence of Implementation:** *Organization participates in a network of trusted relationships with sector partners and government agencies (e.g., Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), Department of Ene*

Cybersecurity Risk Information Sharing Program) for access to timely cybersecurity information

Supply Chain Risk Management

GOAL: Risks associated with control system hardware, software, and managed services are identified and policies and procedures are in place to prevent the exploitation of systems through effective supply chain risk management consistent with best practices (e.g. NIST SP 800-161).

RATIONALE: Commercially available technology solutions (hardware, software, and services) present significant benefits including lower cost, rapid innovation, product feature variety, and ability to choose from competing vendors. However, acquiring these solutions introduces additional risk to the organization because of decreased visibility into how the solutions are developed, integrated, and deployed, as well as the processes to ensure the security, resilience, reliability, integrity and quality of the solutions. The intent of this goal is to ensure that items and services are procured from trusted sources and have traceability through use of a trusted distribution path.

Baseline Objectives

- Ensure control system procurement processes include physical and cybersecurity in acquisition decisions and contract arrangements
  - **Sample Evidence of Implementation:** *Organization policy dictates that all contractual agreements for outsourced control system services have processes for and ensure proper incident handling and reporting, security of interconnections, and remote access specifications and processes*
- Ensure tier one vendors in the supply chain are appropriately vetted to include vendor vetting of their own personnel, vendor vetting of service providers, and vendor vetting of products and software
  - **Sample Evidence of Implementation:** *Organization has a due diligence program to conduct consistent, robust vetting of tier one vendors*

Enhanced Objectives

- Ensure sub-tier vendors in the supply chain are appropriately vetted to include vendor vetting of their own personnel, vendor vetting of service providers, and vendor vetting of products and software.
  - **Sample Evidence of Implementation:** *Organization has a due diligence program to conduct consistent, robust vetting of sub-tier vendors.*
- Ensure vendor-provided software and patches for control systems are reviewed and tested in a safe environment before deployment.
  - **Sample Evidence of Implementation:** *Organization maintains and uses a "sandbox" and test and review vendor-provided software for malicious code or defects.*