National Security Memorandum on Critical Infrastructure Control Systems Performance Goals

National Institute of Standards and Technology
U.S. Department of Commerce

Keith Stouffer, NIST
Peter Colombo, CISA
Vicky Yan Pillitteri, NIST

Overview of the National Security Memorandum

July 28, 2021: President Biden signed a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

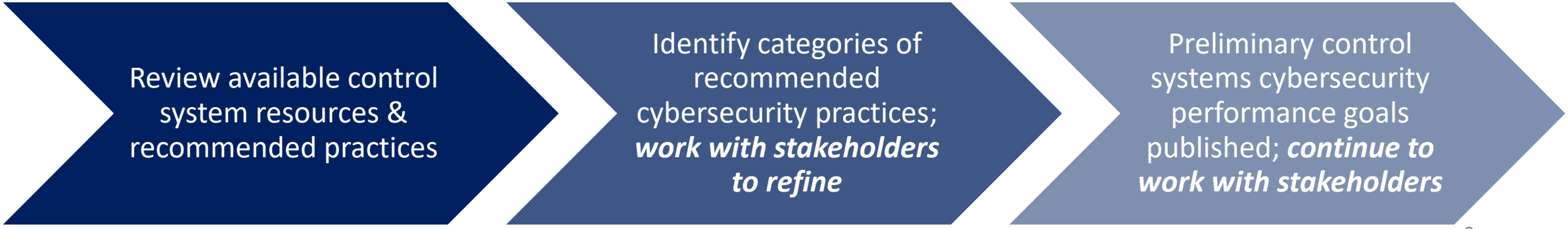
- Section 4 directs the Cybersecurity Infrastructure Security Agency (CISA) and NIST, in collaboration with other agencies, to develop **cybersecurity performance goals** for critical infrastructure that will *"further a common understanding of the baseline security practices that critical infrastructure owners and operations should follow."*
- NSM requires the development of cross-sector control system performance goals and sector-specific critical infrastructure cybersecurity performance goals

  ✓ September 22, 2021: Preliminary control systems cross-sector goals due

  ❑ July 28, 2022: Final cross-sector & sector-specific goals due

Ongoing Interagency and Industry Collaboration

- NSM emphasizes the initiative should be *"a voluntary, collaborative effort between Federal Government and the critical infrastructure community to significantly improve the cybersecurity of… critical systems."*
- CISA and NIST led the development of the draft cross-sector goals with input from interagency and industry control systems groups and delivered them to the White House on September 22, 2021.
  - Control Systems Interagency Working Group (CSIWG)
  - Control Systems Working Group (CSWG)
  - Distribution through the Industrial Control Systems Joint Working Group (ICSJWG)



Intent of the Performance Goals

The Performance Goals are:

- ✓ Baseline and enhanced recommendations on best practices that are consistent across sectors.
- ✓ Intended to draw attention to existing standards rather than replace them.
- ✓ Intended for a broad, cross-sector audience of owners/operators. ***Sector-specific goals will follow.***

The Performance Goals are **not**:

- ✗ A CISA directed compliance regime.
- ✗ Intended to supersede or countermand any existing regulatory guidance or standards.

Preliminary Performance Goals – Issued 9/22/21

Nine preliminary categories of performance goals

- Risk Management & Cybersecurity Governance
- Architecture & Design
- Configuration & Change Management
- Physical Security
- System & Data Integrity, Availability & Confidentiality
- Continuous Monitoring & Vulnerability Management
- Training & Awareness
- Incident Response & Recovery
- Supply Chain Risk Management

Each performance goal includes:

- Description of the goal
- Rationale for the goal

- Specific objectives that support deployment and operation of secure control systems (baseline objectives and enhanced objectives)
- Example evidence of successful implementation

Preliminary Performance Goals

- **Baseline objectives** represent recommended practices for all control system operators.
- **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.
- **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.

Example Preliminary Performance Goal

1. 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 dedicated 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*

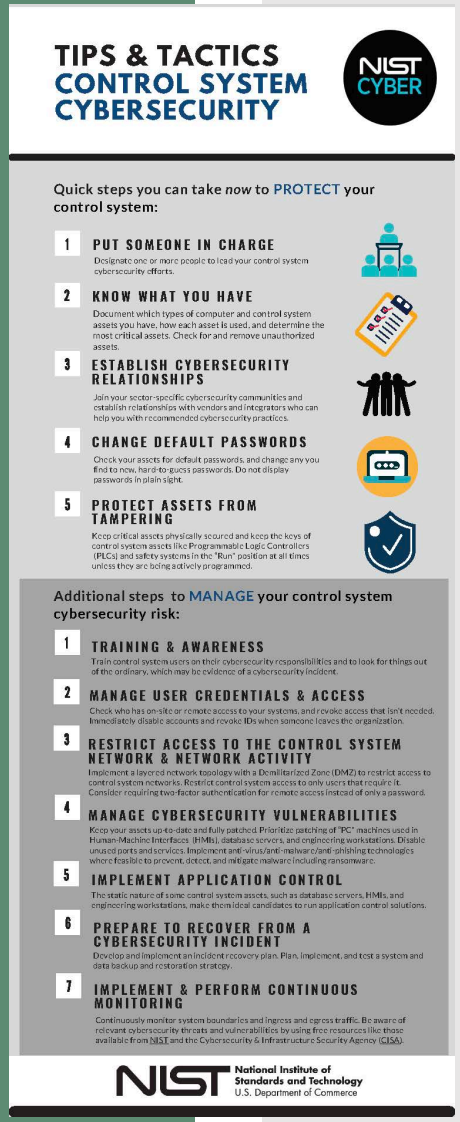
Next Steps

Cross-Sector Goals

- CISA will continue to work with CSIWG/CSWG to refine cross-sector control systems goals, as well as working through Sector Risk Management Agencies (SRMA) and sector coordinating bodies.

Sector-Specific Goals

- CISA is currently conducting internal planning for how to best execute the sequence of activities for developing these goals.
- This will include significant engagement with SRMA's, as well as the wider stakeholder base.



TIPS & TACTICS
CONTROL SYSTEM CYBERSECURITY

NIST CYBER

Quick steps you can take *now* to PROTECT your control system:

1. **PUT SOMEONE IN CHARGE**
   Designate one or more people to lead your control system cybersecurity efforts.
2. **KNOW WHAT YOU HAVE**
   Document which types of computer and control system assets you have, how each asset is used, and determine the most critical assets. Check for and remove unauthorized assets.
3. **ESTABLISH CYBERSECURITY RELATIONSHIPS**
   Join your sector-specific cybersecurity communities and establish relationships with vendors and integrators who can help you with recommended cybersecurity practices.
4. **CHANGE DEFAULT PASSWORDS**
   Check your assets for default passwords, and change any you find to new, hard-to-guess passwords. Do not display passwords in plain sight.
5. **PROTECT ASSETS FROM TAMPERING**
   Keep critical assets physically secured and keep the keys of control system assets like Programmable Logic Controllers (PLCs) and safety systems in the "Run" position at all times unless they are being actively programmed.

Additional steps to MANAGE your control system cybersecurity risk:

1. **TRAINING & AWARENESS**
   Train control system users on their cybersecurity responsibilities and to look for things out of the ordinary, which may be evidence of a cybersecurity incident.
2. **MANAGE USER CREDENTIALS & ACCESS**
   Check who has on-site or remote access to your systems, and revoke access that isn't needed. Immediately disable accounts and revoke IDs when someone leaves the organization.
3. **RESTRICT ACCESS TO THE CONTROL SYSTEM NETWORK & NETWORK ACTIVITY**
   Implement a layered network topology with a Demilitarized Zone (DMZ) to restrict access to control system networks. Restrict control system access to only users that require it. Consider requiring two-factor authentication for remote access instead of only a password.
4. **MANAGE CYBERSECURITY VULNERABILITIES**
   Keep your assets up-to-date and fully patched. Prioritize patching of "PC" machines used in Human-Machine Interfaces (HMIs), database servers, and engineering workstations. Disable unused ports and services. Implement anti-virus/anti-malware/anti-phishing technologies where feasible to prevent, detect, and mitigate malware including ransomware.
5. **IMPLEMENT APPLICATION CONTROL**
   The static nature of some control system assets, such as database servers, HMIs, and engineering workstations, make them ideal candidates to run application control solutions.
6. **PREPARE TO RECOVER FROM A CYBERSECURITY INCIDENT**
   Develop and implement an incident recovery plan. Plan, implement, and test a system and data backup and restoration strategy.
7. **IMPLEMENT & PERFORM CONTINUOUS MONITORING**
   Continuously monitor system boundaries and ingress and egress traffic. Be aware of relevant cybersecurity threats and vulnerabilities by using free resources like those available from NIST and the Cybersecurity & Infrastructure Security Agency (CISA).

NIST National Institute of Standards and Technology U.S. Department of Commerce

Ongoing Development of Technical Guidance and Resources

- NIST continues to conduct the research to develop the initial public draft of NIST Special Publication (SP) 800-82, Revision 3, *Guide to Operational Technology Security.*
- Draft for public comment anticipated in early 2022.

Questions and Feedback

How can CISA and NIST expand stakeholder outreach and coordination to best support the critical infrastructure control systems community?

https://www.cisa.gov/control-systems-goals-and-objectives
https://csrc.nist.gov/Projects/operational-technology-security

Keith Stouffer
keith.stouffer@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov

Peter Colombo
peter.colombo@cisa.dhs.gov