Emerging Cybersecurity Standards for Critical Infrastructure—Lessons from Recent Goals Released by CISA and NIST

October 11, 2021

On September 22, 2021, the Cybersecurity and Infrastructure Security Agency ("CISA") issued its preliminary cybersecurity performance goals for critical infrastructure. These voluntary goals, which were initially announced in President Biden's July 28, 2021 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, represent a non-exhaustive guide of high-level cybersecurity best practices and are intended to support the development of sector-specific performance goals that will be released in 2022.

To create these preliminary goals, CISA, with the assistance of the National Institute of Standards and Technology ("NIST"), identified nine categories of recommended cybersecurity practices. For each category, CISA identified "baseline objectives" that represent recommended practices for all control system operators and "enhanced objectives" for critical infrastructure entities supporting national defense, critical lifeline sectors (*e.g.*, energy, communications, transportation, and water), or "where the failure of control systems could have impacts to safety." Additionally, for each baseline objective, CISA has also provided examples of how organizations can successfully implement the baseline objectives.

While all critical infrastructure organizations should review the technical details associated with the goals, we have outlined the key points of each goal here:

1. **Risk Management and Cybersecurity Governance**. Control system operators can address cybersecurity risks and boost resiliency by identifying and documenting such risks through industry-standard risk assessments, maintaining cybersecurity policies and procedures, and providing dedicated resources—both personnel and budget—to address cybersecurity risk and resiliency.

2. **Architecture and Design**. CISA recommends using established practices for segmentation, zoning, and isolating critical systems to integrate cybersecurity and resilience by design into network architecture. Critical infrastructure entities should consider adopting policies, processes, and technologies to identify risks

during the development process, including by adopting "Zero Trust" architecture if the entity is part of the national defense or critical lifeline sectors.

3. **Configuration and Change Management**. As systems undergo changes and reconfigurations, organizations should ensure that these systems continue to satisfy cybersecurity objectives. Critical infrastructure entities should consider employing documented change management rules to record, maintain, and review standard system configurations in order to more easily detect any changes. Entities can further reduce the risk associated with configuration issues by adopting policies and procedures to ensure factory settings are reviewed and updated to remove unnecessary privileges, and the ability to change control system configurations is limited to approved personnel with a demonstrated need.

4. **Physical Security**. Critical infrastructure entities can protect against physical intrusions to control systems and limit other unintentional damage by restricting physical access to control systems, blocking the use of removable media (*e.g.*, USB devices), and establishing environmental controls, such as temperature and humidity controls.

5. **System and Data Integrity, Availability, and Confidentiality**. The preliminary goals outline a number of baseline objectives intended to protect control systems and the corresponding data against corruption, compromise, or loss, including restricting access to a need-to-know basis, implementing strong password policies, and encrypting data-in-transit and at-rest. Organizations looking to more effectively mitigate these risks should also consider adopting multi-factor authentication for remote access and limiting the data flow between information technology and control system environments, among other items.

6. **Continuous Monitoring and Vulnerability Management**. While monitoring helps entities more rapidly detect and respond to a cybersecurity incident, proper vulnerability management defends against threats by eliminating known security gaps within a network. Consequently, CISA's goals recommend that organizations take steps to improve network visibility and regularly conduct penetration tests and vulnerability assessments of internal and external systems. Organizations should then consider leveraging a coordinated patch management program to remediate identified vulnerabilities and ensure timely implementation of published third-party patches and/or updated software.

7. **Training and Awareness**. An important step towards protecting against and mitigating cyber-attacks and breaches is training personnel to understand cybersecurity concepts and practices so they can recognize control system cybersecurity risks and act within established cybersecurity policies, procedures,

and practices. Critical infrastructure entities should also consider training control system operators and cybersecurity personnel in control systems security at intermediate and advanced levels, including through tabletop exercises.

8. **Incident Response and Recovery**. Organizations can limit the impact of a cyber-attack and minimize recovery times by implementing and testing control system response and recovery plans with clearly defined roles and responsibilities. Critical infrastructure entities should consider developing support networks, including with sector partners and government agencies, among others, to enable more effective incident response.

9. **Supply Chain Risk Management**. Increasingly, threat actors are leveraging vulnerabilities in third-party software and/or compromising vendors, including managed security service providers, to compromise victim networks. CISA recommends identifying risks associated with control system hardware, software, and managed services, and implementing policies and procedures to prevent the exploitation of systems through effective supply chain risk management consistent with best practices.

CISA's goals reflect the beginning, not the end, of what the federal government expects in terms of cybersecurity maturity from critical infrastructure. With this in mind, critical infrastructure entities in all sectors should consider the following key takeaways:

- **The Goals Are Non-Binding**. These goals are just that: goals. They are intended to reflect high-level principles that CISA would like to see critical infrastructure entities achieve. They are not benchmarks, requirements, or a checklist of standards that require immediate action. Instead, they are a non-exhaustive list of best practices that, if widely adopted, would enhance the cybersecurity posture of critical infrastructure writ large.

- **These Goals Are Indicative of Future Regulation**. With that being said, these goals are indicative of future cybersecurity standards or regulations. CISA and other federal agencies will likely build off of these goals when developing binding regulations. Recent legislation, including an amendment to the National Defense Authorization Act passed by the U.S. House of Representatives, directs CISA to establish required cybersecurity standards and conduct examinations to determine compliance. While this amendment is likely to be merged with other cybersecurity legislation in the U.S. Senate, critical infrastructure entities should expect for these goals to reflect future regulations, whether by CISA or sector-specific agencies.

- **The Goals Generally Align with Preexisting Industry Standards**. Notably, because CISA leveraged a range of industry frameworks to identify these goals, they do not

substantially depart from recognized best practices. Thus, if an organization has already aligned itself with the NIST Cybersecurity Framework, the Financial Services Sector Coordinating Council Cybersecurity Profile, or the NERC Critical Infrastructure Protection standards, its cybersecurity program likely has a strong foundation to achieve CISA's goals. Critical infrastructure entities should consider these objectives against what is already in place, and identify any differences as potential areas of growth.

- **Certain Sectors May Receive Heightened Scrutiny**. CISA's inclusion of enhanced objectives indicates that although there are 16 critical infrastructure sectors, those that implicate national defense, livelihood (*e.g.*, water, energy, communications, transportation), or safety may be subject to elevated standards. Even if an organization does not generally fall into one of these categories, companies should consider whether individual lines of business or specific projects or processes fall into these sectors and consider the enhanced objectives accordingly.

Keep in mind that these goals are not exhaustive—they are high-level cybersecurity best practices. CISA plans to conduct more extensive stakeholder engagement as these goals are finalized in the coming year.

We will closely follow developments in this area and provide any updates at the Debevoise Data Blog.

To subscribe to our Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Luke Dembosky
ldembrosky@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

Andres S. Gutierrez
asgutierrez@debevoise.com

SAN FRANCISCO

H Jacqueline Brehmer
hjbrehmer@debevoise.com