Updates
March 23, 2023
Sector-Based Cybersecurity Requirements for Critical Infrastructure, From Our Water Systems to the Skies

Following the release of President Biden's National Cybersecurity Strategy, Acting National Cyber Director Kemba Walden explained that the Biden Administration is "expecting more" from owners and operators in critical infrastructure sectors, embracing the concept of a new cyber social contract advanced by Walden's predecessor, Chris Inglis. That vision calls upon critical infrastructure operators and other major private sector entities to assume greater responsibility for hardening U.S. cybersecurity, even beyond their own platforms. It marks a recognition that cybersecurity, in the face of escalating threats, requires commitment from and collaboration across federal government agencies and their private sector partners.

Several efforts are also underway to address root cybersecurity concerns and develop tools and frameworks that work across sectors. The National Institute of Standards and Technology (NIST) released Special Publication 800-82, a Guide to Operational Technology (OT) Security, which offers guidance on addressing the "unique performance, reliability, and safety requirements" of systems that underpin a number of critical functions. Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which initiated rulemaking procedures that will require critical infrastructure operators to report certain incidents to federal government agencies. And the Cyber Security and Infrastructure Security Agency (CISA) released a set of Cyber Performance Goals establishing a security baseline for both OT and information technology (IT) systems deployed by critical infrastructure operators.

CISA Director Jen Easterly has indicated that CISA plans to coordinate with Sector Risk Management Agencies to build upon the Cyber Performance Goals and provide additional, sector-specific guidance to address risks and measures that are unique to particular industry sectors.

A Sectoral Approach

Only weeks after these announcements, the Environmental Protection Agency (EPA) and the Transportation Security Administration (TSA) have published sector-specific mandates to improve the cybersecurity of public

water and aviation systems, respectively.

Public Water Sources

Just this month, the EPA used existing authority to require states to evaluate the cybersecurity of public water systems. The requirement, which the EPA presented as a "clarification," was released in a memorandum with a number of cybersecurity resources to help operators improve security.

The memorandum notes that a number of public water systems have "failed to adopt basic cybersecurity best practices," which leaves them at risk for cyberattacks "from an individual, criminal collective, or a sophisticated state or state-sponsored actor." Consequently, the EPA will require states as co-regulators to take steps to assess the cybersecurity of any operational technology involved in "producing and distributing safe drinking water." This will involve integrating cybersecurity controls into states' regular public water system sanitary surveys and will leverage state authority to require the closure of identified gaps. The EPA also offers significant federal assistance to achieve these objectives.

Beyond this high-level requirement, the EPA grants significant discretion to states in how to implement the cybersecurity assessments:

- First, states may require the public water system to "conduct a self-assessment of cybersecurity practices" and independently identify gaps using an assessment approach approved by the state;
- Second, public water system operators may alternatively engage a third party from the public or private sector to undertake the assessment (the EPA notes that it is expanding its own capabilities in this area);
- Third, states may opt for surveyors to directly evaluate cybersecurity practices during regular sanitary surveys; or
- Fourth, states that already have other programs for centralizing cybersecurity assessments (e.g., through state homeland security agencies) may lean on those programs, provided that they cover the public water systems and are at least as stringent as the controls identified for the sanitary surveys.

Aviation

Shortly following the release of the EPA memo, TSA announced an aviation-specific cybersecurity amendment, effective immediately for all airport and aircraft operators. The amendment largely mirrors TSA's recent directive for freight railroad and passenger carriers, and focuses on "performance-based requirements."

TSA's cybersecurity amendment seeks to strengthen the aviation sector by enhancing security and preventing unauthorized access to critical systems and data by implementing continuous monitoring, detection, network segmentation, risk-based system patching, and access control systems. Like the rail-facing TSA directive, it focuses on network segmentation policies and other controls that allow the operational technology systems to continue if there is a compromise. The approach also mandates that airports and aircraft operators mitigate exploitation risks by implementing operating system patches based on a risk-based prioritization schedule. Regulated entities must also proactively assess the effectiveness of these measures to detect and respond to cybersecurity threats and anomalies that affect critical cyber systems operations by developing a TSA implementation plan. TSA will then approve and measure the entities' effectiveness against the steps described in the plan.

The new cybersecurity amendment builds upon the previous TSA requirements for airports and aircraft operators, which included measures for cyber incident reporting, incident response planning, and cybersecurity vulnerability assessments. As with the freight and passenger rail security directive from October 2022, TSA has not yet established any penalties for failure to comply with these cybersecurity requirements, but it is possible that penalties will be established in the future.

Advancing the Strategy

These sectoral measures may vary in their substance but generally build upon the Biden Administration's commitments to defending critical infrastructure and shaping market forces to drive security and resilience. Both efforts promote these pillars of the National Cybersecurity Strategy and provide for centralized program development while allowing sector- and operator-specific flexibility and supporting collaboration with private sector operators.

Risk- and Outcome-Based Approaches

The sectoral strategies build in flexibility by embracing risk-based approaches to critical infrastructure security. They focus on identifying desired cybersecurity outcomes and competencies without prescribing how entities must achieve those goals. These methods are distinct from compliance-based approaches, which focus on the implementation of technology-specific controls, and which some critics argue can fail to keep up with evolving technologies and shifting attack vectors. For instance, rather than mandating exactly what cybersecurity controls operators must implement, the EPA provides that state authorities and the operators they oversee may look to a range of frameworks to fulfill their cybersecurity objectives, including CISA's Cyber Resilience Review and the NIST Framework for Improving Critical Infrastructure Cybersecurity. Though the EPA provides a "checklist of recommended cybersecurity practices and controls" along with its memorandum, it notes that they are optional means of identifying and closing cybersecurity gaps.

Similarly, the TSA amendment applies performance-based requirements to airports and aircraft operators. The amendment provides limited, flexible criteria, allowing the aviation sector to prioritize and allocate resources to meet security objectives. This trend of focusing on outcomes allows for innovative and cost-effective approaches tailored to diverse operators' unique circumstances, risks, and resources.

Shared Responsibility

The sectoral mandates further show the Administration's trend toward requiring private-sector operators to share responsibility for the cybersecurity of critical infrastructure systems, which tend to depend on an integrated web of public and private operators, systems, and technologies and are subject to overlapping regulatory authorities. Consistent with that approach, some regulatory schemes adopt a "hub-and-spoke" model, in which a central cybersecurity agency sets core standards and supports more local or sector-specific agencies in developing and deploying more tailored guidelines and capabilities. Public water systems, for example, are run by a diffuse network of roughly 52,000 localized systems, many of which are small and lack sophisticated cybersecurity expertise and capabilities. Accordingly, the centralized capabilities built out by agencies like CISA and the EPA to support assessments and remediations are essential.

A similar recognition underpins the TSA amendment, which tasks airports and aircraft operators with developing and implementing their own cybersecurity plans, while also establishing TSA-led planning baselines and centralized reporting requirements. While the government is still charged with protecting the nation from cyberattacks, owners and operators of critical infrastructure are being charged with a more active role in cybersecurity.

Security Through Resilience

Finally, the new EPA and TSA requirements reflect the twin imperatives of cybersecurity and resilience, embodied within the five basic capabilities of the NIST Cybersecurity Framework:

- Identify organizational systems, people, assets, data, and capabilities behind an organization to understand risk vectors.
- Protect critical services through the development of safeguards.
- Detect cyber events early on through anomaly detection and continuous monitoring and detection processes.
- Respond quickly and appropriately, leveraging incident management planning.
- Recover to normal operations in a timely fashion to reduce impact.

Building up an organization's posture in accordance with these capabilities can help stop attacks from occurring in the first place and also allow operations to continue as normal, where possible, to minimize the impact of a breach. For example, in an Oldsmar, Florida, water facility attack cited in the EPA memorandum, credentials leaked as part of a breach enabled hackers to log into the facility's systems and change the acceptable lye ratios to dangerous levels. While monitoring techniques allowed the systems to detect the issue before any human harm occurred, credential management safeguards can, in some cases, prevent such attacks from getting through in the first place.

TSA's mandate similarly places resilience at its core by driving security mechanisms designed both to prevent attacks and also to enable recovery in the event that attackers get through. Functioning effectively, access controls and vulnerability patching can thwart potential breaches, while network scanning and segmentation enable early identification of threats and allow compromised systems to be isolated, such that operations can continue during a breach. This marks a focus on detection, but also (more importantly) on segmentation, to enable aviation and critical infrastructure to bounce back.

Takeaway

Businesses in the water and aviation sectors should immediately assess whether they are likely to be affected by new cybersecurity rules and consider a legal and technical risk assessment.

Even beyond the public water and aviation sectors, the EPA and TSA rules help illustrate the Biden Administration's new strategy of enhancing the cybersecurity of critical infrastructure systems through outcome-based requirements and provide clues about forthcoming regulatory initiatives for other critical infrastructure sectors. As the National Cybersecurity Strategy moves toward implementation, private critical infrastructure operators will need to heed Associate Director Walden's call to assume a greater role in U.S. cybersecurity, rather than treating it as a government or user responsibility. This will require covered operators to pay close attention to compliance and regulatory developments, which may impose immediate obligations. Critical infrastructure operators should also take advantage of opportunities to engage with regulators to shape the cyber social contract that will ultimately bind them.

Authors

Explore more in

Environment, Energy & Resources | Government Contracts | Product Liability Litigation | Real Estate & Land Use | Data Security Counseling and Breach Response

Related insights

Update

Algorithmic Price-Fixing: US States Hit Control-Alt-Delete on Digital Collusion

Update

SB 6 Implementation Shaping Data Center Future in Texas