ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

A New Flightpath for Cybersecurity

Compliance and Ethics

Government

Information Governance

Technology, Privacy, and eCommerce



Cheat Sheet

Executive Order 14028. The Biden-Harris administration's new cybersecurity rules for federal contractors are tougher than ever and will usher in a new era of best practices.

Reporting. Organizations will need to rapidly report any cybersecurity incidents, which are increasing in number.

Supply chain risk. A key focus of the executive order is neutralizing supply chain risk.

Anticipate and adapt. A new framework is needed so organizations can respond to threats that are moving at warp speed.

The cascade of cyber incidents in 2020 and 2021 shined light on weaknesses some companies and government agencies have in identifying, managing, and responding to cyber threats — and sharing threat information. With the severity of cyber incidents and the costs associated with incident management continuing to rise, the US government, using its purchasing power, appears to be poised to usher in a new approach in cybersecurity best practices, which may affect companies of all sizes and in all industries.

The Biden-Harris Administration Executive Order 14028 (Cyber EO), Improving the Nation's Cybersecurity, sets forth new cybersecurity rules impacting federal contractors and suppliers that are

tougher than ever. The requirements move beyond long-standing and generally accepted compliance approaches and recognize the new challenges of navigating cyberattacks, where threats change quickly and the decision space to react can quickly collapse.

Implementing this new cyber schema will require contractors to examine every aspect of their business, from software purchases to supply chains. Furthermore, companies may need to create the necessary tools so that they can adapt to cyber threats as their businesses become increasingly connected.

But the impact of the Cyber EO is likely to extend far beyond the public sector. President Biden's stated goal is for the federal government to lead the private sector toward improved cybersecurity standards and safeguards overall. The order establishes a framework and direction for what many anticipate will become best practices for the private sector to mitigate evolving and increasing cybersecurity threats. For corporate counsel in the private sector, the requirements can offer a sort of flight path for ways to strengthen your infrastructure and understand your own cyber readiness — from how to better prevent breaches to how to navigate incident reporting.

The order directs procurement and acquisition changes for federal government contractors and suppliers. It is the most impactful development related to the government's cybersecurity requirements since the release of the first public draft of the Cybersecurity Maturity Model Certification (CMMC) in 2019. Over the next year, federal agencies will adopt the wide range of recommendations, rules, and standards the order directs. The most far-reaching changes will impact cyber incident reporting and information sharing; supply chain security risk mitigation; and implementing system hardening practices to strengthen network infrastructure. Here are some key ways contractors will be navigating cybersecurity in the future.

Reporting cyber incidents more rapidly (and likely frequently)

Incident reporting is going to expand and expectations of transparency are going to increase. As part of the new normal, the order aims to extend the requirements on some federal contractors to provide cyber incident information to the federal government. Specifically, the order directs policy changes that will require Information Technology (IT) and Operational Technology (OT) providers to share with their federal government customers information about cyber incidents or potential incidents that could impact government networks.

The order also instructs information and communications technology (ICT) service providers entering into contracts with agencies to promptly report when they discover a cyber incident. To implement this process, the order requires a review and update of the current FAR and DFARS contract requirements.

Defense Industrial Base (DIB) contractors are currently subject to the DFARS requirement to "rapidly report" cyber incidents within 72 hours. The new rapid reporting mandates contained in the order, however, differ from the current reporting requirements for DIB contractors under the DFARS Safeguarding Clause 252.204-7012. Notably, in the current -7012 Clause requirements, contractors have some discretion in determining what qualifies as a "potential cyber incident," enabling some notifications to be made on a "voluntary" basis, while other federal agencies also impose reporting obligations on contractors through contract clauses or policies.

In addition, the reporting obligation in the order, and the order itself, makes no reference to Controlled Unclassified Information (CUI). Consequently, under the order a contractor may be required to report

an incident that had no actual or potential impact on CUI.

To implement new reporting obligations, the order directs changes to the FAR, which include government-wide, mandatory reporting requirements to the Cybersecurity and Infrastructure Security Agency (CISA). While the details regarding this new reporting requirement are yet to be established, the order notes that the time period for reporting “the most severe cyber incidents” cannot “exceed three days after initial detection,” mirroring the incident reporting period currently in the DFARS.

Notably, new requirements under the order may require less rapid reporting for less sensitive incidents. In implementing the requirement, the government may define a “less sensitive incident” as one not involving CUI.

As often happens with new government initiatives, this order may set a course toward enhanced reporting expectations and best practices for companies in a broad range of sectors.

Here are some steps you can consider taking to meet those emerging expectations.

Know what's in your contracts.

Review current contracts with suppliers, customers, employees, and other stakeholders to assess reporting obligations and enhance roles and responsibilities to ensure compliance with those contractual obligations.

Develop compliant and workable incident reporting policies and procedures.

Develop, or enhance as appropriate, your cybersecurity Incident Response Plan (IRP) to include an escalation plan for internal and external reporting in the event of an incident and a protocol for assessing the severity of an incident.

Typically, the team responsible for assessing and implementing reporting obligations will include legal counsel to help ensure all regulatory and legal risks and reporting obligations are contemplated; IT professionals to assess the significance of the event; HR or a company’s privacy office to review obligations for reporting incidents impacting sensitive personal information; and communications professionals to respond as needed to media inquiries.

The IRP should also establish internal paths of communication not only to government regulators and law enforcement, but also internally to senior executives and ultimately to the board of directors.

Train key and responsible stakeholders.

Establish training programs for responsible stakeholders within your company, including tabletop exercises, to “test” their ability to timely report incidents and assess where there may be gaps.

Notably, a tabletop exercise is a useful tool to evaluate interactions among internal stakeholders and simulate interactions with and notifications to external stakeholders, such as government, law enforcement, customers, and suppliers.

Consider taking advantage of US government cyber incident information sharing opportunities.

As part of the government's efforts to increase cyber incident information sharing, which is another key element of the order, you may be approached by US government partners, including the Department of Homeland Security and the Department of Defense.

They may request you enter into information sharing agreements, which sometimes include opportunities to mitigate the risk of reporting cyber incidents. Taking advantage of these opportunities may help you identify, assess, monitor, and respond to cyber threats.

Although the potential impacts of reporting cyber incidents may trigger financial, reputational, and other business risks, the legal risks of not reporting may be more significant. Transparency, honesty, and effective management post-incident is often the key to effectively managing incident reporting obligations.

Evaluate and mitigate supply chain cybersecurity risk

Chief among the motivations underlying the order was what is commonly referred to as the SolarWinds incident. In late 2020, it came to light that the networks of hundreds of entities, including those within the US government and their contracting partners, were potentially exposed because these entities used third-party software that had been surreptitiously hijacked by a foreign adversary.

Simultaneously, the COVID-19 pandemic brought into sharp focus how precariously the US economy and national security had been relying on key industries, especially the ICT industry.

Just weeks after assuming office, the Biden-Harris Administration took its first major step to address these concerns by issuing Executive Order 14017, America's Supply Chains. Among other broad supply chain directives, EO 14017 specifically directs certain agencies to evaluate the risks posed by critical supply chains' reliance on digital products and their associated cybersecurity vulnerabilities.

Months later, the Biden-Harris Administration upped the ante with its Cyber EO, presenting a far more granular proposal focused on software supply chain security in particular. Specifically, the Cyber EO tasks the US government with improving the security and integrity of the software supply chain across the board.

Top among its priorities is shoring up the security of so-called "critical software," defined by the software's relationship with a combination of factors, including whether the software:

- Is designed to run with elevated privileges or manage others' privileges;
- Has direct or privileged access to networking or computing resources;
- Is designed to control access to data or operational technology;
- Performs a function critical to trust; and
- Operates outside of normal trust boundaries.

Common examples of "critical software" thus include those providing services related to identity and access management (IAM), endpoint security, remote access, and backup or disaster recovery.

What remains to be seen is exactly *how* critical software — and eventually other forms of software used in federal networks — must be improved. The order directs the US government to establish new guidelines for software supply chain security before the end of the year, for which industry continues to wait.

Under the order, those looking to provide software to any US government customer will eventually be required to test their source code to minimum standards, attest to their compliance with other forthcoming security requirements, and share certain data about their product security with the public.

Interestingly, in the context of software supply chain security, the order steps beyond the confines of its predominantly federal focus to call attention to the growing call for a broader “security labelling program” for consumer electronics, with a particular focus on Internet of Things (IoT) devices.

Using the order as a guide, private sector companies can begin the process of mitigating software supply chain related risks by considering the following items.

Determine what software is critical to the business.

Starting with the National Institute of Standards and Technology (NIST)’s definition of “critical software,” consider inventorying their current software providers and categorizes the criticality of their services.

In addition to the foundational trust criteria used by NIST, consider the sensitivity of the data that the software is intended to access — or may be granted logical permission to access.

Consider the extent to which the software is necessary to the provision of key business functions.

Consider the relationships between different software. For example, are certain programs developed by the same provider? Does certain software better interact with each other than others, making certain “bundles” of software more important than individual pieces?

Investigate the security behind business-critical software.

After assessing *which* software is most important to your business, dig a layer deeper and probe specific suppliers.

Here, the guidance ultimately provided under the order can prove to be a helpful checklist of considerations. These may ultimately include the providers’ secure development lifecycle processes, their geographic footprints and funding sources, their history of security vulnerabilities, and the transparency behind their products.

This may be done internally and with the assistance of external resources, as the contracting industry has often done when assessing how securely suppliers are handling CUI.

Know the scope of your contractual options.

Perhaps most critical of all is a commitment to act on the information you uncovered about the critical software. It is recommended that you have a process in place to proactively consider the wide range of options at your disposal to address potential shortcomings, including reopening contract negotiations or exploring contractual remedies.

Part of this knowledge is obtained by reviewing and digesting the potentially myriad contract obligations and considering potential supply chain implications (e.g., impact on critical suppliers, etc.).

Having this playbook in advance can help companies quickly assess and execute on the best next steps, depending on the specific risk factors that have been identified.

Harden security practices

At the cornerstone of the order lie system hardening requirements intended to swiftly identify vulnerabilities and enhance network verification requirements prior to accessing secure systems. The order encourages proactive deployment of Endpoint Detection and Response (EDR) solutions aimed at rapidly identifying cyber incidents in addition to cyber hunting. The goal being earlier identification and remediation of network vulnerabilities to help decrease the overall risk exposure to cyber threat actors and their potential theft of sensitive data.

The order also directs the government to implement multifactor authentication (MFA) throughout government systems, requiring users to identify themselves through multiple verification measures, and credentials before traversing federal information systems. Multifactor authentication augments network security by adding protection in layers. The more layers or “factors” in place, the less risk an intruder can access a critical system.

While this system hardening protocol is aimed at government networks, it is likely that these same cyber practices will be expected of contractors, and industry, in turn. These EDR and MFA requirements are already included in various cybersecurity standards, and you should determine what standards are required for your line of business or already legally or contractually required.

Here are some steps you may consider in determining what hardening practices and broader cybersecurity standards work best for your company.

Determine whether your company operates a regulated network.

The data that is processed on your company network or obtained through course of business will determine if you are operating a regulated network subject to federal or international regulations. Often these regulations dictate specific cybersecurity standards that inform information security practices as well as cyber incident reporting requirements.

For example, if you operate business in the European Union, then you are subject to the General Data Protection Regulation (GDPR), and your systems must follow the related GDPR principles. Alternatively, if you process, store, or transmit CUI under a government contract, then NIST SP 800-171 is likely the cybersecurity standard you must follow unless specified otherwise.

If you do not operate a regulated network, consider identifying a standard and mapping to it.

Even unregulated industry may benefit from mapping to an accepted cybersecurity standard. In fact, it is increasingly considered prudent business strategy for unregulated companies to identify and implement an enhanced cybersecurity standard followed by regulated industries.

There are various cybersecurity frameworks that you may consider and some may be more conducive for certain industries based upon their risk portfolio. These include: NIST Cybersecurity Framework (CSF), Center for Internet Security (CIS) Top 20 Critical Security Controls (CSC), NIST SP 800-171, and the Cybersecurity Maturity Model Certification (CMMC).

Mapping to these standards may entail substantial upfront resource costs of time and money. However, these investments often have a significant return. An adequately safeguarded network better enables a company to focus on achieving its business, financial and operational objectives. Additionally, various cybersecurity standards are becoming minimum baselines for entering into business with other companies where information or other critical resources are exchanged.

Pick a standard and follow it.

Technical assessments across the enterprise, penetration tests, and tabletop exercises can help pressure test how well you have implemented your adopted standard and identify potential gaps and vulnerabilities within your IT infrastructure.

> Picking a standard imposes an obligation to follow it.

Charting a new flight path

Although Cyber EO is anticipated to result in cybersecurity improvements for the public sector and offer insights for the private sector on how to better protect businesses and the common public good, it will likely not be the last measure to address the ever-growing cyber risk facing government and industry.

Cyber threat actors continue to grow in sophistication every day. Steering clear of them will require companies to chart a new flight path that will require far more than fulfilling a checklist. They will need to build a framework that allows them to anticipate and adapt, where the way forward is often unmarked and threats are moving at warp speed.

Sean P. Bamford



Associate General Counsel and Chief Privacy Officer

Lockheed Martin Corporation

Sean P. Bamford is the associate general counsel and chief privacy officer of Lockheed Martin Corporation.

Evan D. Wolff



Partner

Evan D. Wolff is a partner at Crowell & Moring, where he is co-chair of the firm's Privacy & Cybersecurity Group. He is a former special assistant to the assistant secretary for infrastructure protection at the Department of Homeland Security.

Kate M. Growley



Partner

Crowell & Moring

Kate M. Growley (CIPP/US, CIPP/G) is a partner in the Washington, DC office of Crowell & Moring.

Maida O. Lerner



Senior Counsel

Crowell & Moring

Maida O. Lerner is senior counsel for Crowell & Moring.

Michael G. Gruden



Associate

Crowell & Moring

Michael G. Gruden (CIPP/G) is an associate for Crowell & Moring. He is a former branch chief/supervisory contracting officer for the US Department of Defense, Pentagon.