Published on *The National Law Review* https://natlawreview.com

The National Cybersecurity Strategy Implementation Plan: What Contractors Need to Know

Article By:

Eleanor M. Ross

Jeffery M. Chiow

Go-To Guide:

- The Implementation Plan describes 65 initiatives to achieve the objectives laid out in the National Cybersecurity Strategy
- Builds on prior cybersecurity policies, including EO 14028, to require contractors to increase IoT cybersecurity, promote accountability in software supply chain security, and implement harmonized cybersecurity and incident reporting standards
- Seeks to shift the burden of cybersecurity from end users to large suppliers and creators of cybersecurity and information technologies
- Highlights the role that the False Claims Act and the Civil Cyber-Fraud Initiative will play in holding contractors accountable for violating regulatory obligations

When the White House first announced its revisions to the National Cybersecurity Strategy in March 2023, it was clear that the strategy would have a significant impact on government contractors. The strategy calls for two fundamental shifts in how the United States will allocate cybersecurity roles, responsibilities, and resources. First, large suppliers and creators of cybersecurity and information technologies must assume a greater share of the burden for mitigating cyber risk. Second, long-term investments in cybersecurity are to be incentivized.

In July the Biden administration announced the National Cybersecurity Strategy Implementation Plan (Implementation Plan), detailing how the government will advance the cyber strategy.

The plan describes 65 initiatives to achieve the objectives laid out in the strategy, and several of them will impact federal contractors.

Implications for Federal Procurement

While the strategy does not specifically focus on federal procurement, it relies and builds on the cybersecurity policy the Biden administration announced in Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity,” and recognizes how the government’s purchasing power can be leveraged to achieve particular outcomes.

Notably, the strategy highlights the use of acquisition regulations to hold government contractors to higher standards of cybersecurity and software supply chain accountability, in the hopes of driving changes in market expectations even beyond federal contracts. It specifically calls for implementing the cybersecurity standards and software supply chain regulations mandated in EO 14028 and discusses accountability measures to ensure compliance with existing and new regulations.

The strategy also emphasizes the Department of Justice Civil Cyber-Fraud Initiative’s role in holding entities accountable for providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cyber incidents and breaches.

The important role contractors will play in furthering implementation of cybersecurity standards is a key tenet of the strategy, and contractors should take note of the increased liability they could face for noncompliance with these standards.

Key Takeaways for Contractors

The Implementation Plan identifies specific actions the federal government intends to take to achieve the goals in these national cybersecurity documents, and how the government will prioritize finalizing the implementation of existing requirements from legislation. The Implementation Plan identifies many critical initiatives; those most relevant for contractors include the following:

- New Cybersecurity Regulations: EO 14028 called for developing new Federal Acquisition Regulation (FAR) regulations addressing cybersecurity incident reporting and standardized cybersecurity contract requirements for civilian agencies. According to the latest regulatory updates, the incident reporting and cybersecurity FAR clauses are currently under review at the Office of Information and Regulatory Affairs (OIRA), which has up to 90 days to complete its review. If OIRA approves the rulemaking, it will be published in the Federal Register. The Department of Defense also sent the Cybersecurity Maturity Model Certification cybersecurity rulemaking to OIRA on July 25, 2023, indicating that the Defense Federal Acquisition Regulation Supplement cybersecurity standards likely will be forthcoming in the fall.

- Internet of Things (IoT): In 2020, Congress passed the Internet of Things Cybersecurity Improvement Act, which called for issuing new FAR regulations governing security measures for IoT devices. The Implementation Plan calls for the Federal Acquisition Regulatory Council to “propose FAR changes in line with” the requirements of this Act. Completion is estimated for Q4 FY23, suggesting that draft regulations could be forthcoming soon.

- Critical Infrastructure: Pillar One in the Strategy is focused on improving the protection of critical infrastructure. The Implementation Plan highlights the ongoing efforts to establish harmonized cybersecurity requirements and incident reporting mechanisms for critical infrastructure. Completion of these efforts is expected in Q2 FY25 and Q4 FY25, respectively.

- Software Bill of Materials and Supply Chain Security: The EO called for a FAR clause

requiring compliance and attestations with applicable secure software development standards developed by the National Institute of Standards and Technology. The draft FAR clause has not yet been finalized, but in the meantime, the Cybersecurity and Infrastructure Security Agency has issued a draft self-attestation form to be used by software publishers. In addition to these requirements, the Implementation Plan calls for advancing a software bill of materials, which would require tracking all the components and dependencies that comprise a piece of software.

- Accountability Mechanisms: The Implementation Plan echoes the strategy's call to leverage the False Claims Act to ensure contractors comply with applicable regulations. The Implementation Plan notes that the Department of Justice will "expand efforts to identify, pursue, and deter knowing failures to comply with cybersecurity requirements in Federal contracts," using the Civil Cyber-Fraud Initiative.

Issuance of these new requirements will take time, and there will be opportunities for contractors to engage with the government, such as via open comment periods. Congressional authorization could also slow implementation.

However, we now have a blueprint for implementing cyber requirements that contractors should carefully examine and continue to monitor. These requirements bring new compliance obligations and with them heightened risks for contractors.

Contractors should have the False Claims Act and the Civil Cyber-Fraud Initiative in mind and be sure to understand their obligations before signing representations/certifications, contracts, options, or modifications containing any new requirements.

National Law Review, Volume XIII, Number 213