SheppardMullin
Government Contracts & Investigations Blog
Latest updates on Developments Affecting Government Contracts & Investigations

Biden's Cybersecurity Executive Order

By Townsend Bourne & Nikole Snyder on May 17, 2021

POSTED IN CYBERSECURITY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

On May 12, 2021, the Biden Administration issued its much anticipated "**Executive Order on Improving the Nation's Cybersecurity**." Below are provisions we believe will be of most interest to contractors, as well as any company that provides information technology ("IT") and operational technology ("OT") services, cloud computing, software, or internet of things ("IoT") technology, as the new regulations and standards called for in the Order are likely to have an impact beyond government contractors.

Sec. 2 – Sharing Threat Information – recognizes **IT and OT service providers, including cloud service providers**, have unique access and insight into cyber threat and incident information.

- The government will focus on removing contractual barriers to IT and OT service providers sharing threat information.

- Within 60 days of the Order, the government will review the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) and recommend updates. Per the Order, "recommendations shall include descriptions of contractors to be covered by the proposed contract language."
- Within 90 days of receipt of the recommendations, the FAR Council shall review and publish proposed updates to the FAR.
- **The FAR/DFARS updates are to include requirements that IT and OT service providers:**
    - **(i) collect and preserve data, information, and reporting for cybersecurity event prevention, detection, and response on "all information systems over which they have control";**
    - **(ii) share data, information, and reporting as they relate to cyber incidents or potential incidents directly with the agency with which they have contracted and "any other agency" deemed appropriate by the Director of OMB (in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence);**
    - **(iii) collaborate with Federal cybersecurity or investigative agencies; and**
    - **(iv) share cyber threat and incident information in industry-recognized formats.**
- Within 120 days of the Order, the government will develop steps to ensure service providers share data with agencies, CISA, and the FBI to assist in response to cyber threats, incidents, and risks.
- The Order states a policy that **information and communications technology ("ICT") service providers must promptly report to the relevant agency (and in some cases to CISA) cyber incidents** involving a software product or service provided to such agencies.
    - Within 45 days of the Order, the government will recommend FAR language on:
        - (a) the nature of cyber incidents to be reported;
        - (b) the types of information to report;
        - (c) protections for privacy and civil liberties;

    - (d) the time frame for reporting (contemplates a graduated scale with the shortest reporting period being 3 days);
    - (e) National Security Systems reporting requirements; and
    - (f) the type of contractors and service providers to be covered.
  - Within 90 days of receipt of the recommendations, the FAR Council shall review and publish proposed updates to the FAR.
- The Order calls for streamlining/standardizing cybersecurity contractual requirements across agencies.
  - Within 60 days of the Order, the government will recommend language to the FAR Council for standardized contract language, considering "the scope of contractors and associated service providers to be covered."
  - Within 60 days of receipt of the recommendations, the FAR Council shall review and publish proposed updates to the FAR.
  - Following updates to the FAR, agencies are to eliminate any agency-specific cybersecurity requirements that are duplicative.

Sec. 3 – Modernizing Federal Government Cybersecurity – requires the government to modernize its approach to cybersecurity, to include prioritizing cloud solutions and Zero Trust Architecture. This section contains multiple directives, including:

- **Within 60 days of the Order, the government will begin to modernize FedRAMP** to include training for agencies, improving communication with cloud service providers through authorization, and streamlining/ automating cloud provider authorization and continuous monitoring.
- Within 90 days of the Order, in coordination with GSA/FedRAMP, the government will develop a new Federal cloud security strategy and related materials.
- Within 180 days of the Order, agencies are required to adopt multi-factor authentication and encryption for data at rest and in transit. Although the Order does not require it, It is likely this eventually will flow to the private sector as well.

Sec 4 – Enhancing Software Supply Chain Security – mandates that the government take action to protect software – with a focus on "critical software" – against cyber-attacks.

- **Within 30 days of the Order, the government will solicit input from various sources, including the private sector, regarding standards, procedures, and criteria for software security (including for a Software Bill of Materials ("SBOM")).**
    - Preliminary and updated guidance will be published by NIST relating to enhancing software supply chain security. Agencies eventually will be required to comply with this guidance.
- Within 45 days of the Order, the government will provide a definition for **"critical software**," which will be used to make a list for agencies of software and software products in use or in the acquisition process that fall under the definition.
- Within 60 days of the Order, the government will publish minimum elements for a SBOM.
- Within 60 days of the Order, the government will publish guidelines for minimum standards for vendors' testing of software source code.
- Within 1 year of the Order, the government will recommend language to the FAR Council requiring suppliers of software to agencies to comply with requirements developed under this section.
- **After issuance of the FAR rule, agencies shall remove software products that do not meet requirements from all IDIQ contracts, FSS contracts, GWACs, BPAs, and Multiple Award Contracts.**
    - Legacy software must comply with the new requirements or be the subject of a remediation plan.
- **Within 270 days of the Order, the government will identify IoT cybersecurity criteria for a consumer labeling** The "criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products."
- **Within 270 days of the Order, the government will identify secure software development practices or criteria for a consumer software labeling "**The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone."

In addition to the above, the Order:

- Establishes a government Cyber Safety Review Board to review and assess significant cyber incidents. This Review Board is modeled after the National Transportation Safety Board, and will meet in cases where there are significant cybersecurity incidents (Sec. 5);
- Requires that the government develop a playbook to standardize agency response to cybersecurity vulnerabilities and incidents (Sec. 6);
- Includes steps for the government to maximize early detection of vulnerabilities and incidents (Sec. 7);
- Calls for the government to improve its cyber investigation and remediation capabilities (Sec. 8); and
- Provides for updates to requirements for National Security Systems (Sec. 9).

Government Contracts & Investigations Blog