CEP Magazine - September 2021
The US government is tightening cybersecurity requirements—so should you

By Kristin Roberts, JD, CCEP

Kristin Roberts (kar0032@auburn.edu) is a Compliance Manager for Auburn University in Auburn, Alabama, USA.

The May 2021 cyberattacks targeting 150 government agencies, think tanks, and other organizations across 24 countries are the latest incidents involving malicious actors attempting to gain access to trusted technology providers and their clients' information.[1] The increase in recent cyberattacks at US agencies, institutions, and companies, along with the mounting risk of foreign influence in federally funded research the last few years, has prompted the US to significantly improve its cybersecurity defense and defense contractor requirements.

Institutions of higher education and private companies, as government stakeholders receiving federal funding for research and development, education, or other purposes, will be held to these higher cybersecurity standards, as well. Your compliance program must be ready, willing, and able to adapt to new federal orders, regulations, and legislation that require your organization to secure the information and activities the federal government has entrusted your organization with.

Executive order on Improving the Nation's Cybersecurity

President Biden signed an executive order May 12, 2021, to improve the nation's cybersecurity and protect federal government networks.[2] The order:

- Recognizes the persistent and increasing threat to the American people's security and privacy that cybercampaigns pose, and the federal government's responsibility to partner with the public and private sectors to ensure that infrastructure is secure to protect against these actions and actors.
- Calls for more transparency and information sharing among information technology and operational technology providers, and the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and other executive agencies in the intelligence community, to prevent, detect, and respond to cyberthreats.
- Requires a commitment to modernization from federal agencies in a move toward zero-trust architecture, secure cloud services, Software as a Service, and other technical safeguards, within a 60- to 180-day time frame. ("Zero-trust architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero-trust security model eliminates implicit trust in any one element, note, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.)[3]
- Focuses on the security and integrity of the critical software supply chain, looking to the National Institute of Standards and Technology (NIST) to establish guidelines, in consultation with the federal government,

private sector, and academia, as well as to potentially recommend a tiered software security rating system.

The order also addresses establishing a Cyber Safety Review Board, improving detection of vulnerabilities and incidents, standardizing the government's response to vulnerabilities and incidents, improving investigative and remediation capabilities, and strengthening national security systems.

Companies and institutions that provide products or services to the federal government, whether it be software, systems, or scientific research, can expect to see these cybersecurity requirements in federal contracts in the coming months, if they have not seen them already. Your organization should be prepared to invest significant resources into strengthening your cybersecurity position to continue to do business with the US government.