Briefing: Executive Order on Improving the Nation's Cybersecurity (TLP:WHITE)

Jennifer Pacenza, REN-ISAC; Anurag Shankar, CACR

On May 12, 2021, President Biden signed an Executive Order (EO) to improve the nation's cybersecurity and strengthen the federal government's operational networks. The EO outlines ambitious measures to bolster cybersecurity defenses through improved network protection and information sharing. These measures only directly impact the federal government but will have subsequent effects on other industries, including higher education, through grants and contracts.

Higher Education's Role

The EO explicitly states that academia (and other industry sectors) will be consulted to develop the tools and best practices for complying with mandated standards, procedures, and criteria. In addition, certain elements of the new policy will be open for public review, so our community of experts will have opportunities to provide input.

Summary of the Executive Order

The Executive Order specifies the following actions:

1. **Remove barriers to threat information sharing between the government and the private sector.**
   - The Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) shall be reviewed to incorporate new standardized language for cybersecurity requirements in all government contracts.
   - Information and communications technology (ICT) providers are required to promptly report incident discovery involving software or products used by federal agencies to CISA, who will centrally collect and manage incident information.

2. **Modernize and implement stronger cybersecurity standards in the federal government.**
   - All US government agencies will adopt multi-factor authentication.
   - Agencies are highly encouraged to move information storage to the cloud and to adopt a zero-trust architecture.

3. **Improve software supply chain security.**
   - Developers and suppliers with federal contracts will conform to standardized security practices, including access control measures such as 2FA, minimize dependencies, encryption, and incident monitoring.
   - The EO stipulates the creation of an "energy star" type of label to allow the government, and the general public, to quickly determine a software's security rating.

4. **Establish a Cybersecurity Safety Review Board.**
   - The Cybersecurity Safety Review Board will be co-chaired by government and private sector leads and may convene for after-action assessments to analyze an incident and create actionable recommendations for improvement.

5. **Create a standard playbook for responding to cyber incidents.**
   - All federal departments and agencies will work from a standardized incident response playbook—that incorporates NIST standards—and set of definitions.
   - All departments and agencies will need to meet a certain threshold for preparation, identification, and mediation of possible threats.

Jennifer Pacenza, REN-ISAC; Anurag Shankar, CACR

6. **Improve detection of cybersecurity incidents on federal government networks.**
   - The EO pushes to improve incident detection by creating a government-wide endpoint detection and response (EDR) system, as well as through improved information sharing.

7. **Improve investigative and remediation capabilities.**
   - Federal departments and agencies will conform to robust and consistent cybersecurity event log requirements.

For More Information

- Executive Order on Improving the Nation's Cybersecurity
- Background Press Call by Senior Administration Officials on Executive Order Charting a New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks
- FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks