JANUARY 19, 2022

FACT SHEET: President Biden Signs National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

Today, President Biden signed a National Security Memorandum (NSM) to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, as required in his Executive Order (E.O) 14028, Improving the Nation's Cybersecurity. This NSM requires that, at minimum, National Security Systems employ the same network cybersecurity measures as those required of federal civilian networks in Executive Order 14028. The NSM builds on the Biden Administration's work to protect our Nation from sophisticated malicious cyber activity, from both nation-state actors and cyber criminals.

Cybersecurity is a national security and economic security imperative for the Biden Administration, and we are prioritizing and elevating cybersecurity like never before. To secure our critical infrastructure, the Biden Administration launched a surge effort to improve cybersecurity across the electric and pipelines sectors which has resulted in more than 150 utilities serving 90 million Americans committing to deploy cybersecurity technologies, and we are working with additional critical sectors on similar action plans. The President issued a National Security Memorandum establishing voluntary cybersecurity goals that clearly outline our expectations for owners and operators of critical infrastructure, and we continue to work closely with the private sector on the importance of prioritizing cybersecurity as a central part of their efforts to maintain business continuity. And internationally, the Biden Administration has rallied G7 countries to hold accountable nations who harbor ransomware criminals, updated NATO cyber policy for the first time in seven years, and brought together more than 30 allies and partners to accelerate our cooperation in combatting cybercrime, improve law enforcement collaboration, and stem the illicit use of cryptocurrency.

Modernizing our cybersecurity defenses and protecting *all* federal networks is a priority for the Biden Administration, and this National Security Memorandum raises the bar for the cybersecurity of our most sensitive systems. This NSM:

- **Specifies how the provisions of EO 14028 apply to National Security Systems.** The President's May 2021 Executive Order required that the government "shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order." Consistent with that mandate, this NSM establishes timelines and guidance for how these cybersecurity requirements will be implemented, including multifactor authentication, encryption, cloud technologies, and endpoint detection services.

- **Improves the visibility of cybersecurity incidents that occur on these systems.** It requires agencies to identify their national security systems and report cyber incidents that occur on them to the National Security Agency, which by prior policy is the "National Manager" for the U.S. government's classified systems. This will improve the government's ability to identify, understand, and mitigate cyber risk across all National Security Systems.

- **Requires agencies to act to protect or mitigate a cyber threat to National Security Systems.** The NSM authorizes the National Security Agency, through its role as National Manager for National Security Systems, to create Binding Operational Directives requiring agencies to take specific actions against known or suspected cybersecurity threats and vulnerabilities. This directive is modeled on the Department of Homeland Security's Binding Operational Directive authority for civilian government networks. The NSM directs NSA and DHS to share directives and to learn from each other to determine if any of the requirements from one agency's directive should be adopted by the other.

- **Requires agencies to secure cross domain solutions – tools that transfer data between classified and unclassified systems.** Adversaries can seek to leverage these tools to get access to our classified networks, and the NSM directs decisive action to mitigate this threat. The NSM requires agencies to inventory their cross-domain solutions and directs NSA to establish security standards and testing requirements to better protect these critical systems.

###