TO: Bret Sychak, Acting Agency Head

FROM: Giao Dinh, Research Assistance

SUBJECT: U.S. Cyber Security

DATE: December 6, 2021

The EINSTEIN program, which was launched in 2004 by the Department of Homeland Security National Protection and Programs Directorate National Cyber Security Division, is otherwise called EINSTEIN (*Privacy Compliance Review for the EINSTEIN Program*, 2012). It was characterized by the Department of Homeland Security. EINSTEIN serves a significant job that functions as an intrusion detection system for computer networks from any cyberattacks attempted by unauthorized, penetrated or compromised agencies to the network gateways of government departments and federal agencies.It provides the Cybersecurity and Infrastructure Security Agency with a representation of the government's understanding of the situation of cyberspace (CISA, n.d.-b). According to an agreement between CISA and federal agencies, the Cybersecurity and Infrastructure Security Agency (CISA) will install a system to record network traffic data on Internet access points.With the provided tools, agencies can analyze all the data they collect by themselves; the data will be shared or passed to CISA’s Security Operations Centers.

EINSTEIN has three phases, EINSTEIN 1, EINSTEIN 2, and EINSTEIN 3 Accelerated, each phase performing a different function. EINSTEIN 1 (E1) records every data packet in and out via the network gateways of the government facility and identifies if there are any unusual changes (CISA, n.d.-a). EINSTEIN 2 (E2) has the ability to detect any potential of cyberattacks before the data passes through the network gateways based on the watch list. EINSTEIN 3 Acceleration will compare the classified data with the watch list and block if there is any threat found.

Using EINSTEIN is legal to monitor all traffic that is coursing in and out of the network gateways of federal agencies 24/7, which allows governments to use a database of known malware to combat threats (Bradbury, 2011; Katz, 2021). In addition, EINSTEIN can be seen as a way to protect government agencies from the risks of cyber-attacks and as a system to protect the Federal Civilian Executive Branch (CISA, n.d.-a). To the Fourth Amendment, there would be no search needed if the to/from lines of emails or the IP addressing data of internet traffic the government used to screen for malicious signatures (Bradbury, 2011). There is an agreement between participants (federal agencies with CISA) about the EINSTEIN program as mentioned above. In order to guarantee or not guarantee, due to large-scale attacks by unauthorized intrusions, all traffic entering and leaving the network gateway needs to be audited to maintain and protect the integrity of critical government computer networks (Bradbury, 2011). In addition, Einstein can help prevent or limit the number of harmful invasions.

SolarWinds is an American software company that develops software and provides system management tools for any companies and organizations that need to help manage networks, systems, and information technology infrastructure around the world (Oladimeji & Kerner, 2021). Orion is an IT monitoring system but also the product of SolarWinds that was hacked by hackers. It was a major event and a serious problem due to the effects it caused on thousands of organizations, which included the United States government. That event was known as the SolarWinds hack. As previously stated, SolarWinds Orion was the IT performance monitoring platform that was hacked by a group named as Nobelium (Russian hacker group). Nobelium hackers used a supply chain attack to inject malicious code into the SolarWinds Orion system, making it easier to gain access to the system. Supply chain attack is one of cyber-attacks that is used to harm the organization by focusing on less secure elements of the supply chain software. Because the Nobelium hacker group can easily access the SolarWinds Orion Platform, they can impersonate SolarWinds customers or customers' accounts. As a result, the virus may get access to system files and legally mix in with SolarWinds activities legally, evading any detection or even by antivirus software. Sunburst was the malicious malware that was deployed, according to Oladimeji and Kerner (2021). Nobelium hackers installed Sunburst in SolarWinds Orion's new batch of software, which was released as an update or patch. SolarWinds sent out Orion software updates without knowing; and customers just installed and updated it without awareness. Thousands of businesses were impacted by the SolarWinds attacks, including government agencies (such as Homeland Security, State, Commerce, and Treasury); commercial corporations (such as FireEye, Cisco, Microsoft, Deloitte, and Intel); and others (such as SolarWinds's partners).

While coping with the Covid-19 pandemic and the new possible crisis caused by the new variant (Omicron), the heat of cyber attacks, triple digit rise in cyber attacks, the flourishing of cybercrime, or the cyber pandemic problem is not abating. When cyber incidents happen, the Department of Homeland Security assists potentially impacted entities; evaluates the possible impact on vital infrastructure; investigates those responsible in coordination with law enforcement partners, and organizes the response (*Cyber Incident Response*, 2021). In order to promote a greater degree of unification efforts and national response to cyber incidents, the department collaborates with other organizations to supplement cyber missions, as well as owners and operators of private sector and other non-federal critical infrastructure.

The Presidential Policy Directive 41 (PPD-41) outlining the roles of federal agencies in responding to significant cyber events. With a set of fourth principles, the PPD-41 that helps in governing how the Federal Government's response to cyber incidents even involves private sector entities or government (*Presidential Policy Directive -- United States Cyber Incident Coordination*, 2016). The Department of Homeland Security is a key federal agency in both the threat and asset response (*Cyber Incident Response*, 2021). The subject of asset response is the assets of the victim or prospective targets of malicious conduct, whereas threat response activities encompass pursuing, discovering, and interrupting harmful cyber entities and activities.

The National Cyber Incident Response Plan (NCIRP) reflects and incorporates lessons that are learned from exercises, cyber events, and policy and statutory updates (such as PPD-41). It also leverages the doctrine of the National Preparedness System and serves as

the primary strategic framework, which helps participants be aware of how federal departments and agencies, as well as other national-level partners, give resources to aid in response activities (*Cyber Incident Response*, 2021; *National Cyber Incident Response Plan*, 2016). The NCIJTF has just published a ransomware factsheet that addresses current ransomware with information on preventive and mitigation measures that assist to decrease risk in the public and private sectors from any of the factsheet's stated infection vectors (*NCIJTF Releases Ransomware Factsheet*, 2021).

In light of hack/breach occurrences such as SolarWinds or other cyber incidents that happened in the United States, the country's present cyber defenses are competent. However, we should continue to update information around the world and any technological changes in our daily lives, because these may be one of the factors that shape or cause any changes in cyberspace. Regarding how to prepare to deal with any cyber incident in the near future, preparation and improvement is the last thing I think of.

References

Bradbury, S. G. (2011). Keynote Address: The Developing Legal Framework for Defensive and Offensive Cyber Operations. *Harvard National Security Journal*, *2*. https://harvardnsj.org/wp-content/uploads/sites/13/2011/04/Vol.-2_Bradbury_Final.pdf

CISA. (n.d.-a). *EINSTEIN*. Https://Www.Cisa.Gov/Einstein. Retrieved November 28, 2021, from https://www.cisa.gov/einstein

CISA. (n.d.-b). *The EINSTEIN Program*. Https://Www.Cisa.Gov/Publication/Einstein-Program. Retrieved November 28, 2021, from https://www.cisa.gov/publication/einstein-program

Cyber Incident Response. (2021, November 16). CISA. Retrieved November 29, 2021, from https://www.cisa.gov/cyber-incident-response

Katz, J. (2021, February 1). *Does Einstein need a post-SolarWinds makeover?* FCW. https://fcw.com/articles/2021/02/01/einstein-rethink-supply-chain-hack.aspx

National Cyber Incident Response Plan. (2016, December). CISA. Retrieved November 29, 2021, from https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

NCIJTF Releases Ransomware Factsheet. (2021, February 5). CISA. https://us-cert.cisa.gov/ncas/current-activity/2021/02/05/ncijtf-releases-ransomware-factsheet

Oladimeji, S., & Kerner, S. M. (2021, June 16). *SolarWinds hack explained: Everything you need to know*. WhatIs.Com. https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Presidential Policy Directive -- United States Cyber Incident Coordination. (2016, July 26). Whitehouse.Gov. Retrieved November 28, 2021, from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident#content-start

Privacy Compliance Review for the EINSTEIN Program. (2012, January 3). Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/privacy_privcomrev_nppd_ein_0.pdf