CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

Request for Information on Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan

Notice of Request for Information

Comments Consolidated by Naval Facilities EXWC

1. Comments to National Science Foundation (NSF) for National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD)..... 1
1.1 Consensus Standards Needed for Designing Resilience into Industrial Control Systems 1
1.2 Cybersecurity is Most Appropriately Viewed as Four Separate Technical Domains .. 3
1.3 Strategic Framing Should Fully Enumerate the Actors 5

1. Comments to National Science Foundation (NSF) for National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD)

1.1 Consensus Standards Needed for Designing Resilience into Industrial Control Systems

Request for Comment: NITRD seeks suggestions for additions or modifications to the 2016 Strategic Plan.

Comment: The concept of resilience was addressed in the 2016 Plan under the defensive element "Adapt." The next Plan revision should extend this by making it a goal to explore ways, such as consensus design standards, to ensure appropriate consideration of resilience in designs of critical systems and products.

Discussion: It is hubris to believe that we will be able to completely eliminate the possibility of successful cyberattack, given that every system must allow legitimate access for administration and that systems generally have networked connectivity. Further, simple failure of complex electronic systems, or even the loss of internet connectivity where this has been made necessary for operation, can represent a significant vulnerability.

The 2016 Plan recognizes the value of resilience, including fail-over to backup or alternate systems and hand-off of key functions to entirely different systems or manual processes. However, products are being fielded that fall short of the stated resilience goal for handoff to manual operation. Indeed, the current trend appears to be to make equipment ever more dependent on automation, electronics, and programming code for operation, with fewer provisions for semi-automated backup operation, or manual operation. Designs have even been suggested, such as a self-driving car that has no steering wheel, that would further extend this trend.

An anecdotal example of failure to design for continued operability upon loss of Internet access was provided by the recent wildfires in Los Angeles and Ventura Counties, California. The Woolsey wildfire severed a key fiber-optic cable and Internet access was lost by many in Ventura County. People reported being unable to ready themselves for evacuation as they could not charge electric vehicles without Internet connectivity. In the charger design at issue, the electricity time-of-use preferences were apparently stored on-line rather than locally and, without Internet connectivity, could not be locally updated or reset to allow immediate charging.

An example of the importance of maintaining capability to operate manually is provided by the hacking, apparently by Russian entities, of Ukraine's power grid in 2016. A Wired magazine article on this hack commented that U.S. power firms are more attuned to cybersecurity, but are also more automated and modern than those in Ukraine—which means they could

present more of a digital attack surface. The article additionally notes that American engineers have less experience with manual recovery from frequent blackouts.

The National Technology Transfer and Advancement Act of 1996, PL 104-113, mandated that the Government would use consensus standards wherever feasible, rather than write their own parallel federal specifications. A NITRD investigation of this topic could consider whether the government should write their own standards, while awaiting development of adequate consensus standards in this area.

Potentially, the area of resilient design could become a design sub-discipline or a recognized extension of existing design disciplines such as “failure mode and effects analysis.”

Resilient design discipline would include physical aspects of security, safety, failure effects analysis, cyber security, and system controls. NITRD review could confirm whether “resilient design” could usefully be considered as a logical extension of cyber security. The goal of this discipline would be to design, not to prevent cyber-intrusion, but to put physical or hard-wired systems in place that would limit the allowed range of operation and thus the damage potential available to the successful cyber-intruder.

Recommendations: Include as an objective of the 2019 Cybersecurity Research and Development Strategic Plan update, the goal to explore ways, specifically including consensus design standards, to ensure the inclusion of resilience in the designs of key systems and products.

References: Wired, July 2017, “How an Entire Nation Became Russia's Test Lab for Cyberwar”
https://www.wired.com/story/russian-hackers-attack-ukraine/

1.2 Cybersecurity is Most Appropriately Viewed as Four Separate Technical Domains

Comment: Cybersecurity is most appropriately described by separate but closely-related and overlapping technical challenges that exist within separate domains. These domains include: (1) enterprise (business and financial) systems; (2) social/communication systems; (3) industrial and building control systems; and (4) product and transportation embedded systems.

Discussion: The issue of cybersecurity is a very broad topic that touches almost every aspect of modern life. Some examples include:

1. Enterprise Systems. These systems store large amounts of high value and potentially sensitive information. These systems are almost always controlled access with a limited number of authorized users and administrators. A data breach of a large enterprise system has the potential to disrupt operations, expose sensitive information (personal identifying information, classified data, and trade secrets), threaten the economic viability of the organization, and threaten public safety.

2. Social/Communication Systems. These systems act as a primary communication hub for millions of people. These systems have minimal access controls to maximize public participation and almost no ability to actually verify that a user is who they claim to be. An unverified user of a social and communication platform has the ability to widely distribute non-attributable and false information that can disrupt the functioning of free democratic societies. If misused these systems can be used by a false-flag operator (troll farm) to manipulate public opinion (e.g. election meddling) or even radicalize a segment of the population. Additionally, underlying data sets often contain highly personal information, photos, and reveal personal networks.

3. Industrial/Building Control Systems. These systems provide automated controls that manage lighting, ventilation, heating/cooling as well as other process functions. Generally, these systems are managed by facilities or building maintenance and very long lived. Consequence these systems often are built upon outdated operating systems or communication protocols that include few cybersecurity features. A hacker could potentially use industrial/building control systems to launch other cyber-attacks (e.g. denial of service), disrupt complex industrial equipment, and potentially destabilize large electrical networks.

4. Product and Transportation Embedded Systems. These systems are embedded in individual pieces of equipment (engines, vehicles, industrial equipment, etc.) that perform complex tasks. They may or may not be connected to the Internet or cloud based monitoring services. Generally, end users would not be authorized access to the underlying software. However, these systems can be compromised at the point of manufacturer by an internal hacker, external penetration, or an organized attempt by the component maker in an attempt to disrupt equipment operations potentially allowing unauthorized monitoring of individuals and organizations or intentionally causing equipment operate in violation of legal requirements, such as for engine emission control devices.

Although each of these subtopics share some basic commonalities such as processing, reporting, and transfer of digital signals, each topic has unique challenges that merit separate consideration of cybersecurity improvements. For example, business systems would rarely if

ever allow access to an unverified user but most current social systems routinely allow users self-verify their identity, geographic location, and other personal information.

Recommendation: The 2019 update to the National Cybersecurity Research and Development Strategy should clearly identify each domain (subtopic) and discuss challenges that pertain to each domain. Technical experts may identify different or additional domain groupings. A separate set of research goals may be justified for each domain.

1.3 Strategic Framing Should Fully Enumerate the Actors

Comment: The Strategic Framing section should include an inclusive exploration of the actors found within the categories of adversaries, defenders, and users. This will help to ensure that cybersecurity R&D efforts consider and address all the potentially important actors.

Discussion: The Strategic Framing section of the 2016 Strategic Plan lists assumptions relevant to adversaries, defenders, users, and technology. It would be valuable to further expand upon what sub-groups are found within these top level categories. For example:

Adversaries. Adversaries will perform malicious cyber activities as long as they perceive that benefits out weight possible consequences.

1. State Actor Adversaries – most often focus on gaining a strategic economic or military advantage. This advantage can be in the form of gathering intelligence to create a future military advantage or destabilizing economic/social infrastructure.
2. Unconstrained External Adversaries - most often focus on economic gain, spreading their ideology, or intimidation.
3. Internal Adversaries - most often focus on intimidation or personal economic gain.

Defenders. Defenders seek to either harden technology systems to make attacks less likely to be successful or proactively take the conflict to the advisory by actively disrupting advisory organizations and infrastructure.

1. Consensus Standards Organizations– focus on development of development of standards for technology development, equipment deployment, and operations.
2. Product Developers – focus on developing products that comply with consensus standards will advancing technology capability and security.
3. Testing Laboratories – focus on testing and verifying that individual components and equipment to verify that product developers comply consensus standards.
4. Law Enforcement Defense Organizations – focus on actively disrupting advisory organizations and infrastructure

User Community. User communities include:

1. Internet/Cloud Hosts – focus on developing and maintaining content for end users.
2. Internet Service Providers – focus on transmission of data between the host and user community.
3. End Users – focus on using available content to make drive decisions and serve customers.

Recommendation: Recommend developing and including a more robust description of various cybersecurity actors and relevant entities. This should help to identify all potential stakeholders in order to ensure their consideration during cybersecurity R&D efforts.