taproot security

Nakia Grayson, NIST August 12, 2016

We welcome this opportunity to offer input to the presidential Commission on Enhancing National Cybersecurity in order to fulfill its mission under Executive Order 13718.

Taproot Security is a private US firm advising clients and policymakers on vital cybersecurity matters. As such, our work touches on all ten areas listed in the NIST RFI:

1. Critical Infrastructure Cybersecurity

Progress in uneven across sectors. Those with a history of cybersecurity regulatory oversight (e.g., financial services) are more mature than others. Current focus on establishment of ISAOs for intelligence sharing has little impact on sectors where such practice was already in place (e.g., FS-ISAC) and thus far has done little to benefit the rest. Intel sharing will have more impact when data sanitization requirements are relaxed and liability immunity is established. Until then the information shared will be of minimal operational value.

2. Cybersecurity Insurance

Cyber insurance arguably disincents companies from focusing resources on prevention. There is a place for low-premium, high-deductible policies to protect SMBs against catastrophic incidents, but they need federal regulation and financial guarantees. High premium policies should be discouraged as they divert funds that would be better applied to improving internal infrastructure.

3. Cybersecurity Research and Development

Cybersecurity R&D in academia sometimes leads to useful real world applications, but often the focus is more on grants and publication than on practical solutions. Most federal grants in this area come through NSF with guidance from DHS. The federal government should involve private sector cybersecurity practitioners as blind judges in the grant approval process.

4. Cybersecurity Workforce

Private and public sectors all face a critical shortage of cybersecurity talent. While positive steps have been taken to increase interest in cyber careers at the high school and college level, they will take many years to have significant impact. Meanwhile visa programs (e.g., H-1B) try to fill the gap, but fall well short. Federal government can help on both fronts. In schools, subsidize cyber scholarships and financial aid, and encourage more colleges to offer NSA-accredited programs. Meanwhile establish a new class of visa for IT workers specializing in cybersecurity, with higher quotas but also more background screening.

5. Federal Governance

Private sector industries designated as critical infrastructure should have meaningful cybersecurity oversight. Recent legislation and executive orders addressed this somewhat by designating sector specific agencies with responsibility for cybersecurity oversight, but there is still inconsistency between sectors. The NIST Cybersecurity Framework can serve as a basis for consistency, but each sector needs more detailed and prescriptive guidance, accompanied by meaningful verification and penalties for non-compliance. The FFIEC's IT Examiner Handbooks, recently aligned with NIST's framework, might serve as a model for other sectors.

6. Identity and Access Management

IAM is one area where public sector may be mature than private, especially defense and intelligence agencies where background screening and identity vetting are robust, along with innovation in multifactor authentication

technologies such as biometrics and smartcards (e.g., PIV). Federal government can help the private sector catch up by. NIST should partner with a standards body to develop its identity and authentication special publications into industry standards (e.g., SP800-63). DOD should encourage DIB suppliers to offer enterprise and consumer versions of identity products. OPM should share background screening best practices (and possibly data if it can be done securely).

7. International Markets

Multinational businesses face a global patchwork of privacy and security laws that vary considerably from one country to the next, as well as nation-specific threats in some places. Basic practices such as background checks can be difficult to implement effectively in some countries. The US government lacks jurisdiction to directly address these challenges, but may include cybersecurity requirements in treaties and trade agreements.

8. Internet of Things

IoT is rapidly creating new cybersecurity and physical security hazards, primarily because manufacturers are unwilling to spend the time or money to make their products even minimally secure. Within the US this can and should be addressed through legislation and regulation to mandate minimum levels of security, safety and privacy. However, since many of these products are manufactured outside the US, these requirements must also translate to import rules.

9. Public Awareness and Education

The US general public has little understanding of cyber threats or how to avoid them. This has worsened in recent years, as a steady stream of widely publicized breaches and incidents has numbed people. Many Americans simply accept poor security and privacy as the new normal. Some federal agencies provide useful cyber education to citizens and businesses, but perpetual "yellow alert" warnings just add to public numbness. Federal government should only communicate practical, understandable, actionable information to the public.

10. State and Local Government Cybersecurity

Some critical infrastructure operators (e.g., many electric utilities) are regulated at the state or local level with little federal involvement. State and local agencies often lack maturity in their own cyber defenses, and have limited ability to oversee anyone else's. Federal government should establish cybersecurity rules and regulatory models those units of government can readily adopt. Federal incentives may be appropriate for critical national infrastructure, but should be accompanied by funding grants to mitigate "unfunded mandate" concerns.

Thank you for your dedication to US cybersecurity and protecting the digital economy.

Sincerely,

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com