Testimony of Dr. Charles Clancy

Before the House Committee on Oversight and Accountability

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Hearing "Enhancing Cybersecurity by Eliminating Inconsistent Regulations"

July 25, 2024

Chairwoman Mace, Ranking Member Connolly, members of the committee,

Thank you for inviting me to testify before you today on a topic of critical national importance. My name is Charles Clancy, and I am a Senior Vice President and Chief Technology Officer at MITRE where I lead science, technology, and engineering for the company. MITRE is a non-profit, non-partisan research institution that operates Federally Funded Research and Development Centers (FFRDCs) on behalf of the U.S. Government. Among other technical disciplines, our team of over 1,500 cybersecurity professionals provide deep expertise across the executive branch, including in support of organizations like the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and U.S. Cyber Command. MITRE's ATT&CK™ framework has become the de facto language between government and industry for describing and combatting cyber threats.

Prior to joining MITRE, I spent nine years as a member of the faculty at Virginia Tech where I held the Bradley Distinguished Professorship of Cybersecurity in the Department of Electrical and Computer Engineering, and served as executive director of what is now the Virginia Tech National Security Institute. I started my career at the National Security Agency leading advanced research and development programs.

It is my pleasure to address this committee.

The practice of cybersecurity has grown organically, driven by need. As the risk, threat, and technologies change, so too does our approach to securing them. The consequence is a set of security standards, process, and tools that seek to counter insecurity in different ways, from different perspective, and with different vocabularies.

The first wave of standards, spurred by Federal Information Security Management Act (FISMA) of 2002[1], was compliance driven and focused on checklists of security controls. The second wave was threat-informed and motivated information sharing. The third wave was risk-based, prioritizing continuous assessment and adaptive security controls. The fourth wave of zero-trust is architecture-

[1] NIST and others have had a range of cybersecurity standards that date all the way back to the Privacy Act of 1974. Here we are only considering the a more modern, Internet-era cybersecurity standards.

driven, recognizing our greater reliance on devices, networks, and cloud infrastructure that may be untrusted.

Umbrella frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 take a holistic approach across business processes, technical controls, risk, and threat. These frameworks can be used as an organizing structure and common taxonomy to talk about regulations but they do not go down to the implementation level.

Regardless, this patchwork can leave regulated organizations with mandatory implementation requirements dealing with a jumble of not necessarily contradictory, but certainly fragmented, overlapping, and inconsistent obligations. While under the hood many of the security controls are aligned, there can be considerable differences in auditing processes, data retention obligations, and incident reporting.

Starting first with security controls, a positive step would be to commission NIST to document the differing security control requirements across different standards. Such an enumeration would help with harmonization as various standards organizations update their requirements over time, and help regulators identify consensus controls that would minimize the burden on their stakeholders. Again this is not a call for *new* standards, but rather illuminating the complexity of today's environment so we can build roadmaps that over time will lead to harmonization, and potentially even consolidation.

Next, is auditing processes. If a standard is mandatory to implement, someone needs to check that it's implemented. This ranges from self-attestation of compliance as part of a federal contract "Representations and Certifications", to rigorous annual inspections by a third party auditor. One concerning trend is efforts to make the NIST Cybersecurity Framework mandatory as part of federal contract terms and other mechanisms, and while this is an admirable goal, the Framework is explicitly voluntary and lacks the necessary metrology to even define compliance, making such attestations meaningless[2]. If you want to make something mandatory, then you need a standard that defines and provides the tools to measure compliance.

Additionally, reciprocity must be harmonized[3]. For example, if someone is ISO/IEC 27001 certified, then that should be sufficient for a regulator looking for SOC 2 compliance. Much like government security clearances: an adjudicator doesn't necessassarily take another agency's conclusion as to whether someone should be granted a security clearance outright, but can waive requirements for conducting reinvestigations or polygraphs if they were completed and adjudicated favorably by another agency in the past few years. No security standard is strictly more rigorous than another, as they often have industry-specific or domain-specific attributes, but there are a common core set of

[2] NIST is in the process of working with critical infrastructure sectors to define sector-specific profiles of the Cybersecurity Framework (https://www.nist.gov/profiles-0). Such profiles could provide the necessary context and granularity to define risk-based metrics for compliance assessment. Particularly as CISA deploys Cross-Sector Cybersecurity Performance Goals (CPGs), having these profiles complete is an important precursor to CPGs mandating framework compliance (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals).

[3] MITRE recently recommended greater reciprocity among security standards as part of our Cloud Safe Task Force. https://www.mitre.org/news-insights/publication/cloud-safe-task-force-recommendation-roadmap

requirements across most, and the job of an auditor or regulator can be greatly simplified if there is reciprocity for that common core.

Data retention obligations is another area of complexity. Increasingly, European Union regulations that focus heavily on privacy require data deletion, while U.S. policies including defense acquisition, Sarbanes-Oxley banking regulations, and state-level healthcare regulations requires retention of certain personal information for multi-year periods. Perhaps this falls more into the bucket of harmonizing privacy standards, and is beyond the scope of this hearing, but remains an issue for many organizations.

Lastly is incident reporting, which is the biggest headache for regulated organizations. I personally experienced this earlier in the year when my company, MITRE, was attacked by a Chinese nation state threat actor. We had reporting obligations to over ten federal agencies, all on different timelines, with differing types of data solicited, and most presuming we had all the answers a few hours into an incident response. The reality was that it took weeks, working with two leading third-party incident response firms, to forensicly trace the threat actor's moves through our system to identify with any degree of certainty which agencies' data may have been impacted. In the meantime all we could tell many concerned agencies was "maybe".

The biggest step to helping harmonize these issues would be to have a single clearinghouse for reporting an incident, either operated within a federal agency such as CISA[4], or by an independent third party on behalf of the federal government[5]. The clearinghouse identifies a lead agency to engage with the affected party, and the lead agency would be responsible for coordinating with others across the interagency as appropriate. The clearinghouse could serve a number of other important purposes as well, including: (1) energizing a federal cyber action team to help the impacted organization with incident response, if appropriate and necessary; (2) serving as a focal point for major vendors and cloud providers who may be stakeholders, particularly in widescale cyber incidents; and (3) being an important repository of cross-sector data on adversary cyber operations.

Reporting should be viewed as iterative. As reporting timelines get shorter and shorter, the amount of high-confidence, reportable information collected by the affected organization gets smaller and smaller[6]. We must balance reporting timelines, practical detail on the incident from the impacted organization, and the utility of that data to a regulator. Reporting "we might have been hacked, but we're not sure, and have no idea what may have been impacted" in eight hours to a regulator doesn't provide anything actionable. If that regulator's typical response time for assigning a case agent and soliciting additional information is two weeks, then what was the point of the eight-hour timeline?

[4] The pending implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, will require certain entities to report cyber incidents and ransomware payments to CISA, and likely provides a roadmap for a broader clearinghouse. CISA is in the process of reviewing comments received during the public comment period in developing the Final Rule.

[5] MITRE recently recommended a similar clearinghouse as part of our recent presidential transition paper on Cyber Defense. https://www.mitre.org/news-insights/publication/dont-trust-verify-strengthening-us-leadership-safeguard-our-cyber

[6] The Department of Energy's DOE-417 process is an example where one can report a potential problem and correct the record later if needed.

A clearinghouse could also help with State, Local, Tribal, and Territorial (SLTT) government reporting and coordination. SLTT governments have a growing set of cyber reporting obligations, and a federal clearinghouse could ease the burden on an impacted organization.

In conclusion, I urge the committee to move from study to action. The National Cybersecurity Strategy identified the need to establish an initiative on harmonization. The Peters-Lankford bill currently in the Senate involves years of pilots. National Security Memorandum (NSM) 22 calls on DHS to develop a plan for harmonization in critical infrastructure by April 2025. Last fall's Office of the National Cyber Director (ONCD) Request for Information (RFI) gathered broad information from industry and other stakeholders[7]. We have a good handle on the issues, and need to move out on solutions.

Thank you.

[7] MITRE's response to the ONCD RFI: https://www.mitre.org/news-insights/publication/mitre-cybersecurity-regulatory-harmonization