Eric Mill

Thank you to Chairman Donilon, Vice Chairman Palmisano, and the other distinguished members of the Commission for inviting me to appear here today.

I work at the General Services Administration, where I have served as a policy advisor for GSA's Technology Transformation Service and a software engineer on its 18F team. My comments today are my own, and do not necessarily represent the entirety of GSA, but I hope that they can offer the Commission some practical perspective.

My work at GSA includes a strong focus on information security policy and practice in the federal government. This means not only developing policies that improve federal information security, but developing new software tools to support policy implementation, and working directly with agencies to identify and resolve technical issues.

Today, I want to share a few suggestions from my work in the federal government. They are each simple in concept, but also challenge core assumptions and operations in federal agencies.[5]

First, federal agencies must recruit and elevate active technical practitioners within their organization. Employing staff with active technical skills is absolutely necessary in order for agencies to control fundamental aspects of their information security posture.

This means hiring engineers, penetration testers, and other technical specialists to perform technical functions in-house. Today, this is something that many federal agencies -- even agency IT offices -- often simply do not do. Instead, many agencies largely outsource technical analysis, engineering, and deployment tasks. The growth of "digital services" teams in federal agencies has made a positive impact on bringing technologists into government, but these teams are not usually tasked with performing key agency IT management or information security functions.

However, simply hiring technical specialists is not enough. For the public service to get the most value from its technical staff, and for its technical staff to get the most value from their public service, practitioners must have the autonomy to set agency strategy and to implement modern solutions, and must be given a voice on agency-wide and government-wide decisions.

This requires agencies to make real investments in their technical staff, and for their formal hierarchy to contemplate placing practitioners in senior positions with broad mandates to directly improve agency IT and information security, without necessarily requiring these positions to be supervisory. It also requires that agencies integrate their technical staff into internal and government policy-making processes. Just as agencies call upon their legal staff to provide more than rote analyses of legal risk, agencies should become accustomed to relying on their technical staff when making strategic decisions.

Second, the federal government must drastically change its approach to information sharing. Overwhelmingly, federal agencies default to severe restrictions on sharing documentation, policies, data, and software with the public -- and, in effect, with other agencies.

The federal government is terrifically large, and effecting real change is not always possible through top-down policies and chain-of-command coordination alone. To change how the federal government operates, it is necessary to share information and technology in the widest and most organic ways possible. In practice, the most effective way, by far, for information to have government-wide impact is for it to be distributed publicly.

---

5 These recommendations also apply to policy-making and oversight bodies, such as executive offices, legislative agencies, and offices of inspectors general.

In its comments to the White House on its then-proposed source code policy, 18F described this problem as it relates to software code2 (emphasis added):[6]

> We have consistently seen that the most effective way to share information, software, and experience among agencies is the ongoing public release of data, code, and documentation. Managing and guarding access to "private" software and information consistently entails significant operational overhead when compared to sharing public information. The bureaucratic overhead of secrecy can sometimes be extreme, depending on the scale and temperament of the collaborators. However, this overhead is frequently discounted or unobserved by teams that default to working in private.

Source code is just one example. Agencies can share their technology and security practices without releasing sensitive information. This includes releasing software documentation, sharing agency-wide security policies, publishing technical blog posts, and speaking at conferences about internal practices. As part of this, agencies should become comfortable speaking about their failures and incidents, and how they responded and learned from them. These are some of the critical mechanics that allow the technology industry to rapidly evolve and to have its lessons and best practices spread throughout its community of practice.

This will require greater trust between agency communications and legislative affairs teams and other agency components. Oversight bodies, such as inspector general offices and congressional committees, should encourage this information sharing and should work collaboratively with agencies to resolve security incidents and internalize their lessons.

This may be an uncomfortable transition for some agencies at first. However, if the federal government's security practices are to keep pace with a changing world, this must become the norm for the federal government.

Third, federal agencies need to be reducing their dependence on their network "perimeter", and to avoid unnecessarily centralizing their resources.

Increasingly, maintaining and relying on a trusted network -- whether for a single agency or for multiple agencies -- is in stark conflict with broader trends in the technology industry and the information security community. This conflict can create major inefficiencies in government operations, as well as misalignment of security resources.

The most obvious conflict is that the federal government is under strong practical, policy, and economic pressures to move to "the cloud" -- that is, to rely on computing resources that are beyond their direct control. The benefits of commercial cloud services are numerous, but their use requires placing trust in third parties. These cloud services themselves often have many of their own business relationships with other cloud service providers. Trust is managed through legal agreements, and through software and security mechanisms that limit the amount of trust that needs to be placed in connected third parties. This trend moves agency resources out of agency-controlled locations, while making it easier to support a mobile federal workforce that can access agency resources from any network. This makes reliance on a perimeter increasingly less necessary and less worthwhile.

There is also a clear trend in the information security community towards assuming that components will suffer compromises, relying on privilege separation to limit the effect of compromise, and generally avoiding large central points of failure. Unfortunately, there is a strong tendency in the federal government to centralize resources, such as by creating small numbers of entry and exit points in networks. Limiting the number of network entry points in this way, while conceptually straightforward, places unrealistic security expectations on those entry points. These can lead to

---

6 https://github.com/WhiteHouse/source-code-policy/issues/73, "Open source by default". A public comment by 18F on what eventually became https://sourcecode.cio.gov.

unrealistic security models inside federal agencies, leading staff to rely too heavily on a "trusted network" and failing to require proper privilege separation.

Fundamentally, the path forward for technology and security to scale in the modern world is to rely on logical barriers (software) rather than physical barriers (the perimeter). This means that agencies should broadly be moving away from intranets, and investing in software-based solutions to privilege management.

These recommendations describe a public service that is:

- Supported by a community of technical practitioners with the mandate and ability to make their agencies leaders in information security,
- Accelerating its collective progress by routinely and publicly sharing the work of its staff among the federal community, and
- Has the technical skills to build a modern decentralized infrastructure based on realistic threat models and an embrace of contemporary security trends.

I believe that the above captures how today's most successful technology organizations function, and describes a federal government that can take care of itself.

Thank you again for the opportunity to comment, and for the Commission's important work on improving our nation's security.