December 2018

Bad Idea: Creating a U.S. Department of Cybersecurity

Suzanne Spaulding and Mieke Eoyang

A lack of cybersecurity can have serious consequences – the theft of money or data, an interruption of operations or essential services, or even the compromise of weapons systems or destruction of critical infrastructure. It's no wonder that people are desperately on the hunt for policy solutions to improve the security of systems on which we rely. And while some ideas are better than others, one truly bad idea is to create a Department of Cybersecurity—a hugely disruptive bureaucratic solution that not only fails to solve problems but adds new ones.

The success of a cybersecurity solution requires clarity about the problem that one is trying to solve. As we look at particular challenges, many already have an approach suited to the problem, and none of them involve a Department of Cybersecurity. Let's run through a few of them:

Protecting the U.S. Government from Cyber Attacks

Cybersecurity is an essential element of any government agency's mission. Each government agency has a responsibility to secure its own systems as a part of managing their overall risk. Turning cybersecurity entirely over to a centralized department runs the risk of a one-size-fits-all technical solution that does not recognize that the State Department, the Department of Defense, the IRS, and the Department of Energy each operate in unique risk environments. The cyber landscape is so pervasive and interconnected with real-world operations; one cannot entirely divorce cybersecurity from the implementing functions of all the agencies without losing operational expertise in the mission space that is essential to fully assessing and mitigating risks from cyber.

Common baselines are necessary, and shared tools and cybersecurity services can improve efficiency and common situational awareness. But the Department of Homeland Security already has the authority to set

standards through Binding Operational Directives, enforced by the Office of Management and Budget, and deploys common tools across the civilian government that improve cybersecurity and provide joint situational awareness.

Decoupling ultimate cybersecurity responsibility from the existing Cabinet departments also—perhaps counterintuitively—weakens accountability. Cabinet-level officials should be accountable for ensuring that they can perform mission-essential functions for the nation. Effective cybersecurity is a key aspect of that mission assurance. Removing these IT functions from their implementing agencies and consolidating them in a single department means that those who are responsible for the cybersecurity of systems can't be held accountable by their agency heads, but instead report to someone else.

Coordinating Government Efforts

Take one look at the current cybersecurity landscape across government, and it is clear that coordination is essential. There is a continuing need to eliminate redundancy, improve alignment, and define clearer lanes in the road, but a standalone agency is going overboard and won't solve this problem. Ultimately, the White House will always need to lead coordination efforts between Cabinet-level departments. Empowering a senior level coordinator, either within the Executive Office of the President or nested within an existing body, would meet the need for improved coordination without introducing excessive bureaucracy from a standalone agency.

Potential models that don't require a brand-new agency already exist. The Obama administration installed a White House Cybersecurity Coordinator, which the Trump administration has since uninstalled. If a more robust staffing structure is determined to be needed, one could adapt the model of the Director of National Intelligence, who does not have a department or responsibility for most intelligence operational efforts. Instead, these capabilities remain resident within the agencies whose missions they support.

Protecting the Private Sector from Cyber Attacks

Protecting the private sector from cyber-attacks requires public-private cooperation to address common threats and mitigate potential consequences. Government can promote adoption of best practices by the private sector; share information about threat vectors, vulnerabilities, and mitigation; and discourage lax cybersecurity enforcement practices. This is the mission of DHS, now being implemented by the newly established Cybersecurity and Infrastructure Security Agency (CISA).

We already have an existing structure of Information Sharing and Analysis Centers (ISACs), each established by private sector entities voluntarily seeking greater collaboration and supported by DHS and other federal and state agencies. And Congress created even greater incentives for sharing information with the passage of the Cybersecurity Information Sharing Act, clarifying DHS' role as the central point for information sharing with the private sector, states, and civilian federal government.

Perhaps most importantly, standing up a Cabinet-level cybersecurity department creates a technology stovepipe that moves us away from the holistic cyber-physical approach to protecting critical infrastructure that the private sector and government increasingly understand as essential. Managing cyber risk starts with understanding that risk, which requires understanding the impact or consequences of a cyber disruption. In the federal government, cyber risk must be incorporated into managing the overall risk environment to mission effectiveness. Similarly, businesses must view cyber as part of their overall enterprise risk management. This is not a task ideally suited to the IT wizards who would staff a cyber department—or the IT staff of a business.

Your IT staff is probably no more likely to be able to tell you the impact on your business of a cyber intrusion than the electrician can tell you the impact on your business if the power goes out for an extended period of time. The impact we care about is not the damage to the IT infrastructure but the disruption of the functions that infrastructure enables. Assessing the potential impact of malicious cyber activity means understanding the consequences to business, including reputation and continuity of operations. The kind of expertise DHS has built up over the years for many sectors, and the expertise resident in the sector-specific agencies like Energy and Treasury, is essential and would not be incorporated into a Cybersecurity Department.

Imposing Consequences on the Attacker

Further, the government can go on the offensive and take steps to impose consequences on those who orchestrate cyber attacks. While the discussion often focuses on the technical means that can be used to impose consequences, behind every malicious cyber attack is a human being who directed, planned, or executed the attacks. And while important private-public partnerships can help identify these attackers, only the government has the authority to charge and, ultimately, punish the malicious actors. But we do not need a new Department of Cybersecurity to ensure that this happens. Investigators at the FBI, Secret Service, and other agencies; prosecutors at the Department of Justice; and diplomats around the world are working together to identify, stop, and punish the attackers. These efforts can and should be emphasized and improved, which is why Third Way recently established its cyber enforcement initiative. But these efforts would not be served by wrenching them from their current agencies and cobbling together a new department.

Even if one still believed that the creation of a Department of Cybersecurity was necessary, the process of implementing that solution would make the problem substantially worse. A reorganization of all the different component parts of various cybersecurity-focused missions in other agencies into a single department would disrupt ongoing and critical functions for years while the new agency found its feet. The Department of Homeland Security, created in 2002, is still working on Unity of Effort. And it took years to achieve the stand-up of the Cybersecurity and Infrastructure Security Agency. Taking that away from DHS—which would likely mean ripping it apart to take the cyber element while leaving the all-hazards Infrastructure Protection piece—to combine it with other agencies would disrupt the progress that has been made so far and set it back at a time when threats continue to move forward.

We recognize that the magnitude of the threats posed by malicious cyber activity leads people to look for a big, bold, visible sign of change. Creating a new department is not the answer. We cannot stovepipe thinking about cybersecurity into one centralized place or approach. The threat is so pervasive and so severe that it requires a recognition that a change in thinking is necessary for everyone operating an enterprise – from the app developer in their dorm room, to the mission or business operator, to the President of the United States.

Suzanne Spaulding is a senior adviser to the Homeland Security Program and International Security Program at the Center for Strategic and International Studies in Washington, D.C. Mieke Eoyang is Vice President for the National Security Program at Third Way in Washington, D.C.