The Heritage Foundation

ISSUE BRIEF

No. 4734 | JULY 12, 2017

NIST Is a Standard-Setting Agency, Not a Regulator

Paul Rosenzweig

Congressional House Republicans have introduced a proposal to make the National Institutes for Standards and Technology (NIST) responsible for cybersecurity audits across the government.[1] The idea is flawed in many respects—most especially because asking NIST to do an audit is asking them to do something they simply have never done before. Congress should look for a different organization to take the lead, such as the Department of Homeland Security (DHS).

Cybersecurity in the Federal Government

First, the obvious: The federal government does a poor job at cybersecurity. After the 2015 Office of Personnel Management (OPM) breach, nobody should doubt that our federal systems are no more secure than those in the private sector.[2]

That is precisely why the Trump Administration's executive order on cybersecurity[3] calls for each federal agency to conduct a risk-mitigation assessment of its own cybersecurity. And in doing so, the federal agencies have rightly been told to look to the NIST Cybersecurity Framework[4] to determine how well they are doing.

The NIST Framework was first produced in 2014 and was the product of a year-long standard-setting and evaluation process that was led by NIST scientists, but which incorporated input into the best practices for cybersecurity from all across government and the private sector. It established a baseline of practices ranging from the technical (how best to install firewalls) to the administrative (how best to account for all devices on your network). The Framework, which undergoes periodic revision, sets a minimum consensus-level bar for cybersecurity throughout America. It is far from perfect—but it is an excellent tool by which to measure an enterprise's cybersecurity preparedness, and the Trump Executive Order was right to look to the NIST Framework for a broad-based federal standard.

Indeed, the process for assessing the nation's security seems to be moving forward as one would anticipate. In the immediate aftermath of the executive order, NIST posted draft guidance for federal agencies advising them on how they could align the cybersecurity framework with their current mandates under the Federal Information Security Management Act and assess their security posture. That document was closed to public comments on June 30 and will be published shortly.

As contemplated by the Trump Executive Order, once federal agencies have conducted a self-assessment, that assessment will, in turn, be reviewed by the Department of Homeland Security and the Office of Management and Budget (OMB, which is responsible for much of the federal IT structure). They will "jointly assess each agency's risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination)."

This paper, in its entirety, can be found at
http://report.heritage.org/ib4734

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

NIST, by contrast, has never done an audit in cybersecurity and is traditionally thought of as a cooperative, standard-setting agency. Think of them as an independent body of scientific experts who are responsible for a fact-based assessment of a technical or scientific problem. As a result, NIST has historically advised agencies on cybersecurity. But audits for compliance are typically done by the Government Accountability Office and agency inspectors general—now with another independent review by DHS and OMB.

NIST Audit Proposal Goes Astray

The Republicans on the Science Committee in the House of Representatives are not content with this state of affairs. They introduced a bill, the NIST Cybersecurity Framework Assessment and Auditing Act, that would task NIST with auditing and verifying that agencies have proper cyber protections in place and reporting on laggards. The bill passed[5] out of the House Science Committee in March but has yet to come to the floor and does not have a Senate equivalent.

There are several serious problems with this proposal.

First and foremost, the bill asks NIST to do a job for which it is not equipped. NIST is a standard-setting agency that has no operational experience at all. Having no audit experience and no staff of that sort, asking NIST to conduct detailed audits is simply using the wrong tool for a task. It also muddies NIST's position of auditing compliance with the same standards that it has taken a part in developing. Putting NIST in the position of auditing an organization's compliance with NIST standards could place NIST in an irreconcilable conflict of interest, if, for example, someone plausibly argued that they had mistakenly chosen an improper or wrong standard.

Second, giving NIST an oversight role of any sort would erode its current standing as a neutral, technical arbiter and standard setter. Today, federal agencies and private-sector actors are comfortable with a process of standard setting in which NIST convenes and coordinates but does not adjudicate compliance. That model works well—both in the cybersecurity realm and in a host of other areas in which NIST is responsible for identifying the "right" answer. Imagine how much more reluctant stakeholders will be to share candid assessments with NIST if they anticipated that the next step in the process would be NIST's assessment of them against those candid assessments. This proposal would chill cooperation between NIST and those to be audited by NIST.

Finally, this would further diffuse and disaggregate congressional oversight of the critical issue of cybersecurity. Rather than having yet another agency, with yet another congressional overseer, involved in the problem, Congress should be moving in the opposite direction to consolidate its review as a way of asserting better direction and control of the government's response.

In addition, NIST itself has concerns. In late June of this year, members of NIST's Information Security and Privacy Advisory Board expressed their serious concern[6] about changing the agency's mission. They argued, convincingly, that it would likely degrade NIST's ability to perform its core duties.

Supporters will argue that *somebody* needs to be doing these audits on a government-wide basis

1. NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, H.R. 1224, 115th Cong., 1st Sess.
2. Riley Walters, "Continued Federal Cyber Breaches in 2015," Heritage Foundation *Issue Brief* No. 4488, November 19, 2015, http://www.heritage.org/cybersecurity/report/continued-federal-cyber-breaches-2015.
3. The White House, Office of the Press Secretary, *Executive Order: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal (accessed July 6, 2017).
4. U.S. Department of Commerce, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed July 6, 2017).
5. Joseph Marks, "NIST as Enforcer? House Committee Passes Bill to Expand Agency's Responsibilities," Nextgov, March 1, 2017, http://www.nextgov.com/cybersecurity/2017/03/nist-enforcer-house-committee-passes-bill-expand-agencys-responsibilities/135805/ (accessed July 6, 2017).
6. Joseph Marks, "NIST Cyber Advisors Anxious Over Auditing Agencies," Nextgov, June 28, 2017, http://www.nextgov.com/cybersecurity/2017/06/nist-cyber-advisors-anxious-about-auditing-other-agencies/139062/ (accessed July 6, 2017).

and that agency inspectors general are too diffuse a group for the task. While this concern has some merit, the right response is to identify an appropriate operational agency for the responsibility. Without prejudging a final answer, the natural home for such a task would be at DHS—strongly assisted by NIST expertise, but with its own organic capacity to conduct cyber assessments.

Getting Cyber Roles and Responsibilities Right

Rather than making NIST pick up a completely new responsibility for auditing government cyber practices, Congress should:

- **Empower review of government cybersecurity.** Other agencies, such as DHS, would be better suited for monitoring government cybersecurity. DHS is already responsible for protecting the ".gov" domain and was tasked by President Trump's cyber executive order to review the cybersecurity assessments conducted by each government agency. Congress should ensure that whichever organization takes on this responsibility has the capabilities and legal authority necessary to effectively monitor government cybersecurity practices.

- **Keep congressional oversight of cybersecurity focused.** Principal oversight of cybersecurity issues should not be further fragmented. Doing so would increase the confusion among cybersecurity agencies with inconsistent guidance from Congress.

Improving Government Cybersecurity

The problem is real: Federal cybersecurity is not as good as it should be. And there is a real, substantial need for a government-wide assessment of the problem and a government-wide action plan for reducing the threat. The House Science Committee is to be commended for identifying the problem—as is the Trump Administration. NIST, however, is the wrong tool for the job.

*—**Paul Rosenzweig** is Visiting Fellow in the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*