

The logo for Nextgov, featuring the word "Nextgov" in white, sans-serif font on a green rectangular background.

Nextgov


A stylized graphic of a globe with glowing orange and yellow lines representing data connections or network paths. The globe is tilted, and the lines are dense and overlapping, creating a sense of global connectivity and digital infrastructure.

The New Administration's **CYBER STANCE**

PRESIDENT DONALD TRUMP BEGINS SHAPING FEDERAL CYBERSECURITY

Introduction



 (Cover) 3alex/istock

During his first press conference since being elected, Donald Trump pledged to launch a “major review on hacking” within his first 90 days in office, declaring, “we have no defense” and “we’re run by people that don’t know what they’re doing.”

Weeks into his presidency, Trump is working to make good on his promises to improve the nation's cyber posture. Although much of Trump's cyber agenda remains murky, we've seen executive order drafts that would order reviews of the nation's cyber vulnerabilities and capabilities, and task agency leaders to modernize aging, unsecure systems.

The administration may not start from scratch: Experts are optimistic the president will build on recommendations from a cyber review his predecessor Barack Obama ordered after the Office of Personnel Management breach.

Trump's vow to better federal cybersecurity

will be a challenge, but some former Obama administration officials believe Trump is the right man to take more of an active part in defending industry networks from cyberattacks.

Keith Alexander, former National Security Agency and U.S. Cyber Command chief, was among the cybersecurity experts who met with Trump and former New York City Mayor Rudy Giuliani following the inauguration to discuss early-stage plans for a major government push on cybersecurity. Alexander told *Nextgov's* Joseph Marks he was impressed with how Trump took advice and asked questions.

“I think, if the nation could have sat in and watched it, they would have said, ‘that’s our president; that’s what we need done,’” Alexander said. “I’m very upbeat based on that.”

Camille Tuutti

Nextgov Executive Editor

45 Briefed on 44's Cyber Commission Recommendations

Officials remain bullish the Trump team will draw from their suggestions.

By Joseph Marks

As the first inklings of President Donald Trump's cyber policy emerge, experts remain hopeful team Trump's policy will draw from the Obama administration's heavy lifting.

In particular, there's significant optimism that dozens of recommendations from a major cyber review Barack Obama ordered in the wake of the Office of Personnel Management data breach may be taken up in a 90-day cyber review Trump has promised but not yet formally launched.

That hope has a number of things going for it. Most importantly, Congress and the American public are in full-blown crisis mode over cybersecurity, especially Russian-government backed cyber meddling during the 2016 election.

However, there's one great caution against expecting the Trump administration to take lessons from the Obama team: Donald Trump.

The two administrations clashed mightily over those Russian-backed election hacks, which intelligence agencies say were partly aimed at aiding Trump's election. During the transition, Trump declared the government has “no [cyber]

defense” and is “run by people that don't know what they're doing” when it comes to cybersecurity.

That conflict could make it difficult for Trump officials to openly endorse the commission's findings.

Experts remain hopeful, however, that the Trump team will use the report from the Commission on Enhancing National Cybersecurity as a guidepost—even if they don't give the commission much credit.

“The Trump administration can reframe it in its own words and adopt it as its own initiatives,” said Alan Chvotkin, executive vice president of the Professional Services Council and a former longtime Hill staffer. “They'll apply the Trump administration philosophy, strategy and approach, but that doesn't undercut the work the commission has already done.”

New America Senior Fellow Peter Singer was more blunt: “It would be great if they plagiarized these [recommendations],” he said.

It's not uncommon for administrations to draw on their predecessors' work without acknowledging its origin, which some cyber watchers hope will happen here.

This particular report could be particularly compelling because its recommendations—including increasing cooperation between government and the private sector, and focusing on incentivizing companies to improve cybersecurity rather than regulating them—are largely nonpartisan and align with Republicans' free market preferences, Singer said.

“CYBERSECURITY IS NOT A PARTISAN ISSUE. The commission itself was very substantive and nonpartisan. Some key members have relationships with key leaders in the incoming administration and they can talk to them about some ideas.”

KIERSTEN TODT, *executive director of Commission on Enhancing National Cybersecurity*

The cyber commission co-chairs spent two hours briefing a cross section of the Trump transition team on their report before the inauguration, Executive Director Kiersten Todt told *Nextgov*.

The group that received the briefing included transition representatives for the Defense, Homeland Security, State and Commerce departments as well as the National Security Council and the General Services Administration and a cross-agency technology team, Todt said.

The team also included Joshua Steinman, an executive with the cybersecurity firm Thin Air who has worked with the Pentagon’s Silicon Valley outpost and who is expected to lead Trump’s White House cyber efforts, she said.

“They were thoughtful and constructive and asked great questions,” Todt said. “They have an interest in taking a look at the [report’s] recommendations and which make sense to pursue.”

The report includes a slate of 60-, 100- and 180-day goals for the Trump team related to securing the internet of things, improving public-private cooperation on cybersecurity and beefing up the cyber workforce.

Though appointed by Obama, commission members mostly hailed from industry and academia and several were recommended by Republican leaders in Congress. Todt has stressed several times since the election the commission’s recommendations were designed to fit either the Clinton or Trump administrations and that the commission even eschewed describing particular roles or titles with the presumption either administration might rejigger them.

“Cybersecurity is not a partisan issue,” Todt said. “The commission itself was very substantive and nonpartisan. Some key members have relationships with key leaders in the incoming administration and they can talk to them about some ideas.”

It remains unclear, however, what role the cyber commission report, which was widely expected to be a blueprint for cybersecurity if Hillary Clinton had won, will play in Trump’s 90-day cybersecurity review.

That uncertainty is magnified by questions about the review itself.

Trump suggested soon after his election the review would be led by DOD and later that the intelligence

community would play a leading role. Either of those might undercut DHS' role as lead government liaison to the private sector in cybersecurity.

Trump announced soon before taking office that former New York Mayor Rudy Giuliani would advise him in a private capacity on cybersecurity and help convene a rotating collection of private-sector officials to discuss the topic. It's not clear what role that group will play in the larger cyber review.

Depending on the review's focus, the cyber commission report could be more or less relevant, said Herbert Lin, a commission member and senior research scholar for cyber policy at Stanford University's Hoover Institution.

"Our review focused on the digital economy so if the administration wants to address the role of offensive operations in cyberspace, our report isn't going to be particularly influential," Lin said.

"If Clinton had won, the reception would have been a more favorable one, but that's not to say that this is an unfavorable one," Lin added. "It's just that we don't know yet. The jury's out."

Even if the recommendations are not implemented as part of the 90-day review, that won't be game over, Singer said.

"Sometimes, these reports get utterly buried, but the ideas are out there in the firmament and, for the most part, they're nonpartisan," he said. "So you can imagine many of them popping up in future reform proposals."

There's also the possibility of a cyber crisis—the sort the Obama administration faced numerous times—pushing the Trump administration to implement something fast and looking to the report's recommendations for guidance.

"If there's a major event," Singer said, "that changes the politics of what's possible." ^N

Agency Cybersecurity to Start at the Top

Early executive order drafts hold agency leaders accountable for breaches.

By Mohana Ravindranath

President Donald Trump delayed signing an executive order that would make the heads of federal agencies accountable for internal IT modernization and cybersecurity of their agencies.

Trump was scheduled to sign a cyber-focused executive order Jan. 31 after a meeting with various cyber experts. The White House canceled the signing and Deputy Press Secretary Stephanie Grisham offered no explanation.

An early draft of the executive order creates review boards to examine various aspects of the nation's cybersecurity vulnerabilities, adversaries and workforce, led by the secretaries of Defense and Homeland Security, national intelligence director, and the director of the National Security Agency.

The White House's morning briefing hinted at several changes from the draft. For one, the executive order will

direct heads of federal agencies to take responsibility for internal cybersecurity and for modernizing their organization's technology. The agency leaders should not delegate these tasks to chief information officers, a White House official said.

The measure will direct agency heads to work with the assistant to the president for intergovernmental affairs and technology initiatives Reed Cordish to coordinate those efforts. The director of the Office of Management and Budget will then be tasked with managing and overseeing risk across all components in the executive branch, the official said.

Trump plans to hold cabinet secretaries and agency heads "totally accountable for the cybersecurity of their organizations, which we probably don't have as much as we need," he said during a meeting that included his cybersecurity adviser and former mayor of New York City Rudy Giuliani.

He also plans to "empower these agencies to modernize their IT systems for better security and other uses," spanning federal networks and data, he said.

Agencies protecting civilian networks and infrastructure aren't "currently organized to act collectively/ collaboratively, tasked, or resourced, or provided with legal

authority adequate to succeed in their missions,” a draft of the executive order said.

“[M]aking it clear that the head of the agency is responsible for the systems and the data is helpful,” Rep. Jim Langevin, D-R.I., and head of the House Cybersecurity Caucus, said.

“One of the things I was really upset about with the OPM breach is the director or the agency clearly didn’t understand the value of the data they were charged with protecting,” he added, referring to a massive intrusion into the Office of Personnel Management background checks that exposed the personal information of about 22 million people.

Langevin warned that agencies will need to be given resources to protect their data.

Under Barack Obama, a handful of lawmakers introduced legislation intended to promote IT modernization, including the Modernizing Government Technology Act. The MGT Act proposed that each agency create a working capital fund for modernization and that the General Services Administration operate a broader fund that agencies could apply to for additional support. The bill passed the House, but after the Congressional Budget Office estimated the cost at \$9 billion, it didn’t get traction in the Senate.

Broad IT modernization “won’t be satisfied with a reshuffling of organizational charts,” Rep. Gerry Connolly, D-Va., said in a statement emailed to *Nextgov*. He said he hoped the new administration would be willing to invest in

cybersecurity and IT upgrades by “leveraging savings,” as the MGT Act intended.

Trump noted during his meeting with Giuliani that agencies need to work with the private sector, which is “way ahead of government” in cybersecurity capability, to make sure owners and operators “have the support they need from the federal government to defend against cyber threats.”

“Broad IT modernization won’t be satisfied with a reshuffling of organizational charts.”

REP. GERRY CONNOLLY, D-Va.

Despite the fact that the Democratic National Committee spent “hundreds and hundreds of millions of dollars more money than we did,” they were hacked “terribly successfully,” Trump said during the meeting. “And the Republican National Committee was not hacked. Meaning it was hacked, but they failed. It was reported, I believe, by Reince [Priebus] and other people that it was hacked, but we had a very strong defense system against hacking.”

Giuliani noted that the private sector is “wide open to hacking, and sometimes by hacking the private sector, you get into government. So we can’t do this separately.” ^N

The New Federal Hiring Freeze Could Hurt Cyber Recruiting

Retaining the talent already in agencies will be key.

By Mohana Ravindranath

On his first official day in office after inauguration, President Donald Trump has made good on his plan to institute a federal hiring freeze—part of his effort to slash the federal workforce.

Trump has said there would be exceptions for the military, and a White House memo notes the freeze would be waived “when necessary to meet national or public safety responsibilities.”

Some experts fear a temporary hiring freeze could exacerbate a chronic problem in the federal government: a widespread shortage of cybersecurity talent.

A hiring freeze could signal to essential cybersecurity talent—especially those who might consider joining the public sector from higher-paying industry jobs—that there’s no need or desire for them in the federal government, Alan Chvotkin, executive vice president of the Professional Services Council, told *Nextgov*.

And it could have a “number of potential negative repercussions, including growth in contractors that are making important technical decisions that the federal government should be making,” former White House



Pablo Martinez Monsivais/AP

Deputy Chief Technology Officer Nick Sinai told *Nextgov*.

Many federal officials have discussed a dire, but not currently quantified, dearth of cybersecurity talent, especially in the wake of the massive breach of the Office of Personnel Management system that compromised the background check information of more than 22 million people.

Barack Obama’s White House unveiled an ambitious Cybersecurity National Action Plan last year, which allotted \$62 million to investing in cybersecurity education

“Citizens demand a lot of government, and the new administration has talked a lot about improving the services citizens get. **OUR GOVERNMENT CAN’T DO THAT WITHOUT IT TALENT.**”

MALLORY BARG BULMAN, *the Partnership for Public Services' director for research and evaluation*

nationwide, eventually to bolster the federal cybersecurity workforce. Trump’s cybersecurity plan outlined a general intent to “[o]rder an immediate review of all U.S. cyber defenses and vulnerabilities, including critical infrastructure, by a Cyber Review Team of individuals from the military, law enforcement and the private sector.”

Before her term ended, former OPM Acting Director Beth Cobert led an ambitious effort to ramp up cybersecurity recruiting. Under her tenure, OPM began working with the Homeland Security Department to create a better “human resource management system for its cyber workforce,” according to her exit memo. That effort aims to help hiring managers be more flexible in hiring processes and pay to onboard cyber talent.

Cobert had also promoted an “excepted hire” system, called the Cyber Civilian Hire Service, which would help tech professionals switch government jobs without entering a new competitive process. Cobert advised against a hiring freeze in an exit interview with *The Washington Post*.

The federal government’s IT employees skew older, meaning the technology workforce could attrit rapidly

if faced with a hiring freeze, Mallory Barg Bulman, the Partnership for Public Service’s director for research and evaluation, told *Nextgov*. There are almost three times as many IT specialists over 60 years old as there are under 30, she said.

For agencies that have a high percentage of retirement-eligible cyber employees, it’s essential to make sure the ones who remain are engaged, Bulman said.

“IT specialists within government tend to report lower levels of engagement than other workers,” she said. Agencies who want to retain cyber talent during a hiring freeze should devote resources to training and retaining those employees.

“Citizens demand a lot of government, and the new administration has talked a lot about improving the services citizens get,” she added. “Our government can’t do that without IT talent.”

The hiring freeze also requires the Office of Management and Budget to create a long-term plan, within 90 days, for cutting the federal workforce. ^N

Election Systems to Remain Critical Infrastructure—For Now

DHS secretary give early hints that the administration may keep the controversial designation.

By Joseph Marks

Homeland Security Secretary John Kelly wants to continue treating election systems as critical infrastructure, retaining a controversial designation made late in the Obama administration, he told lawmakers Feb. 7.

Kelly's predecessor Jeh Johnson designated federal and state election and voting systems as critical infrastructure during the final days of the Obama administration despite objections from some state officials who worried about a federal power grab.

Critical infrastructure is an official DHS designation that comprises 17 industry categories, including chemical and power plants, transportation systems and dams.

Johnson's move came days after then-President Barack Obama imposed additional sanctions on Russian intelligence agencies and officials for hacking Democratic political organizations in an effort to aid the electoral chances of

President Donald Trump and to damage Democratic nominee Hillary Clinton.

"I believe we should help all of the states, provide them as much help as we can to make sure their systems are protected in future elections, so, I would argue that, yes, we should keep that in place," Kelly said of the designation during a hearing on border security before the House Homeland Security Committee.

That designation makes it easier for DHS to provide grants and other funds to state election systems to ward off physical and cyberattacks. Cyber experts from the U.S. and other nations have also endorsed a rule of the road for international cybersecurity that states critical infrastructure should be off limits from cyberattacks.

Kelly was less bullish on the designation in advance of his confirmation, saying in a questionnaire that "the notion that DHS can or should exercise some degree of influence over state voting systems is highly controversial and appears to be a political question beyond the scope of DHS' current legislative cyber mandates."

While U.S. officials have long feared a destructive cyberattack on critical infrastructure, only a few are known to have occurred, including the U.S.-linked Stuxnet attack on Iran's nuclear program, the Iran-linked attack on a Saudi oil company and the Russia-linked attack on Ukraine's power grid. ^N

What Former NSA Chief Keith Alexander Thinks of Trump's Cyber Plans

Alexander's bullish on Trump applying his business-savvy to government problems.

By Joseph Marks

Former National Security Agency Director Gen. Keith Alexander wants government to take a more active role defending private-sector networks from cyberattacks and he thinks President Donald Trump can help make that goal a reality.

Alexander was one of several cybersecurity experts who met with Trump and former New York City Mayor Rudy Giuliani shortly after the inauguration to discuss early-stage plans for a major government push on cybersecurity.

Alexander declined to provide details about the closed-door portions of that meeting, but told *Nextgov* he was impressed with the new president's demeanor and his interest in the issue.

"I was impressed with the way he took on advice and came back with questions," Alexander said. "I think, if the nation could have sat in and watched it, they would have said, 'that's our president; that's what we need done.' I'm very upbeat based on that."

He also hopes Trump will allow the Defense and Homeland Security departments to pivot from responding to private-sector breaches and cyberattacks after they happen to more actively preventing adversary nation-states

and other cyberattackers from penetrating U.S. companies' networks in the first place.

"Here's the question: Is defense of the country incident response or preventing an attack?" Alexander said. "In the [Obama] administration, it was incident response. That means after the attack. That means, the missile landed and blew up the city and now, we're in there cleaning up. If that's your city, you'd say, 'we'd like to stop that missile' and that's what we should be doing [in cyberspace] in my opinion."

Industry, however, has been hesitant to share the sort of information about its internal networks that would allow government to help repel an attack before it happens—partly because of concerns about government surveillance prompted by NSA information shared by leaker Edward Snowden.

Legislation signed by Obama in 2015 shielded companies from legal liability in exchange for voluntarily sharing cyber threat information with the government and nevertheless took many years to pass.

Nextgov spoke with Alexander on the sidelines of the RSA Cybersecurity Conference in San Francisco. The transcript that follows has been edited for length and clarity.

Nextgov: President Trump has said he wants to make government cybersecurity a major priority. What should he do?

Alexander: If you were to step back and look at government

at large, the biggest problem that you see is antiquated infrastructure, IT staffs that are not fully resourced with the best talent, departments and agencies struggling to maintain the competence levels that they need.

Especially on the civilian side of government, the first thing that comes to mind is, if we were a corporation, how would you start to consolidate? I assume that we'll walk down the road.

Nextgov: Government has attempted to consolidate IT numerous times in the past and run into a lot of stumbling blocks.

Alexander: This is where President Trump will come in. It's a business decision. If we were running government like a business, we'd do this. It's the logical thing to do and you'll save money and get better security. So, get on with it. Departments and agencies will say, 'I don't want to do this because I don't want this guy to run my stuff.' The reality is, get over it.

Nextgov: It sounds as if you're bullish on Trump's business experience making a difference.

Alexander: Everybody has some levels of reservation, but I'm bullish because I think he's going to approach this— [and this is] why he was elected—as a business person vs. a politician. You want to save money? You want to do a better job? Here's how you do it. Wha-chhhh! [Karate chops the air.] Everyone says, 'well, there's political things.' 'I'm not looking at politics. If you're running the government like a business, you'd do it today.'

Nextgov: Will this mean more opportunities for cyber and IT contractors?

Alexander: I think those opportunities will probably remain consistent. The key would be those firms that can see the vision of where you've got to go.

Nextgov: Do you expect something that goes beyond consolidating and improving IT and security?

Alexander: Step two would be, OK, what's the role of government?

There's actually two sets of roles and responsibilities for government: to protect themselves and their data and to protect the nation. You have to have a mechanism of sharing information that can go at networks speed— information about attacks that are coming in at networks speed that the 'defend the nation team' can see.

Nextgov: Does that mean more cyber threat information sharing between the Homeland Security Department and critical infrastructure?

Alexander: It actually goes far beyond that. What's DHS' job?

Nextgov: To protect the nation domestically?

Alexander: No, DHS' job is actually incident response and to set standards. DOD's job is to protect the nation. If the nation is under attack, DOD is supposed to respond, but DHS is the ones that sees [the attacks].

Nextgov: But there are gray areas like the Sony breach where DHS is the lead response agency because they don't reach the level of armed attacks against the U.S.

Alexander: I'm not a constitutional lawyer, but when you read the preamble to the Constitution, there's a phrase in there: 'provide for the common defense.' You and I believe, as physical people here, that we're protected from a foreign army coming in and shooting us. If a foreign power were to come in and destroy our infrastructure with bombs, should our military protect us? Yes. Now, what about when cyber is a prelude to that first step?

Nextgov: Do you think DOD should play a larger role in domestic cybersecurity?

Alexander: That's where the administration has to sort out the rules of engagement. The real question is, should the constitution be re-written 'for the common defense of some, not all, not you Sony and not you Target? If you're hit by nation-state actors, well, sorry, good luck with that?' No. It's the common defense. And it's hard, but it's doable.

Nextgov: There was an early sense Trump might pivot to relying more on the military for domestic and critical infrastructure cybersecurity. Should he do that?

Alexander: I don't know where specifically he'll come down on that. I think what he'd say is, 'how's it going to work? Show me how you're going to defend the country?'

I think the administration is wrestling with this. My experience, in sitting down with the president, is he was very thoughtful. He asked great questions. I saw a version of the president I thought the rest of the nation needs to see.

Nextgov: Are you concerned either the hiring freeze or the administration scandals so far will get in the way of the Trump administration accomplishing what you want it to?

Alexander: No. With the hiring freeze, the question is how much government do you need. The new heads of departments and agencies need to come in, look at what they have, where they can save, what they should do. That's a good thing to do.

On the second part, I have no greater insight than you do on that. I think they're going to do the right thing. Standing up a new team in government, even if you have 60 days to prepare, you can't do all of it.

It's in our best interest to see this country doing good and we should be doing the best we can to help the current administration, whether we voted for him or not, accomplish what's good for our country. It seems to me that the rhetoric that was pre-election continues. My comment

is: Wouldn't it be better if we argued over how we help government get it right?

Nextgov: Do you think the concern about Gen. [Michael] Flynn [who recently resigned after acknowledging discussing sanctions relief with Russian officials before Trump's inauguration] was a result of pre-election rhetoric?


Alexander: I wasn't in the team in there. I've met him and knew him from before, but I didn't work directly with him. I suspect that he did that for the good of the administration.

Nextgov: Should he not have resigned?

Alexander: I don't know. I don't know what went on the room, so it's pure speculation. I will tell you, by and large, the team he's selected are really good people.

Nextgov: The government presence at cybersecurity conferences has risen since you came to Black Hat in 2013 in the wake of the [Edward] Snowden leaks. Is that a good thing?

Alexander: It's a good thing. This is not two nations, an industrial nation and a government. It's 'one nation, under God, indivisible' and we haven't done that. We've missed that in our approach. The government is here not for the government. It's for the people and for industry. The more government reaches out, the more it talks to industry, the better it is and what industry and the people want is for the government to protect our nation.

We should be cheering them on like we do at the Olympics instead of nitpicking them like we do today. We're running around fighting with each other and the bad guys are throwing arrows at us. We should be thinking about what we can do to fix government, defend our country, work with our allies. Do you think terrorists stopped and said: 'They've got a new team in there. Give them a few months before we come in. Give them an even chance.' That ain't happening. Same thing in cyber. 

About the Authors



Joseph Marks

Joseph Marks covers cybersecurity for *Nextgov*. He previously covered cybersecurity for Politico, intellectual property for Bloomberg BNA and federal litigation for Law360. He covered government technology for *Nextgov* during an earlier stint at the publication and began his career at Midwestern newspapers covering everything under the sun. He holds a bachelor's degree in English from the University of Wisconsin in Madison and a master's in international affairs from Georgetown University.



Mohana Ravindranath

Mohana Ravindranath covers civilian agency technology and IT policy for *Nextgov*. She previously covered IT for *The Washington Post*, and her work has also appeared in *Business Insider* and *The Philadelphia Inquirer*. She is a graduate of the University of Pennsylvania.