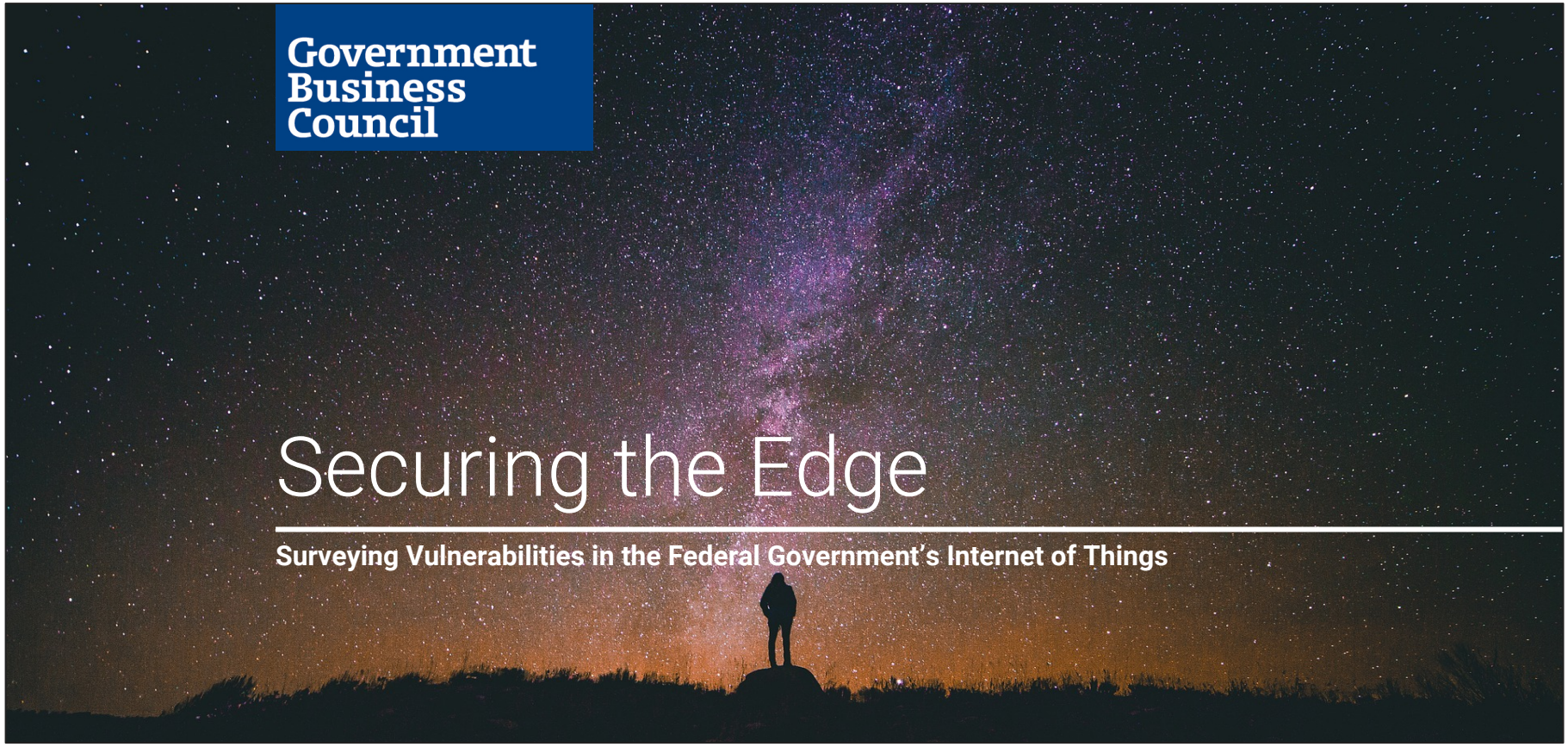


Government Business Council

Securing the Edge

Surveying Vulnerabilities in the Federal Government's Internet of Things

Underwritten by

BROCADE

March 2017

Table of Contents

Overview

Purpose

In October 2016, vulnerabilities in Internet-connected devices enabled hackers to overload server traffic from a leading web services provider, temporarily shutting down Internet access across large parts of the eastern United States.[1] The attack was the latest example of the dangers facing the Internet of Things (IoT), the vast network of physical objects and sensors being used to transmit data and automate basic functions. This is especially true in government where employees increasingly rely on IoT devices to transmit sensitive, mission-critical information from remote locations around the world. While the White House has pursued aggressive cyber policy in the past year aimed at minimizing network vulnerabilities, current procurement processes and outdated security architectures threaten to wind back the clock, placing agency data and their devices in the line of fire.[2]

With the IoT now on pace to exceed 30 billion units by the year 2020[3] — and public sector IoT growth poised to surpass private sector adoption rates by 2019[4] — the U.S. government's next steps are critical. In order to find out what federal leaders are doing to secure the data on the devices in their own agencies, Government Business Council (GBC) on behalf of Brocade undertook an in-depth research study in January 2017.

Methodology

To assess the perceptions, attitudes, and experiences that federal leaders have regarding security of the Internet of Things, GBC deployed a survey to a random sample of federal respondents in January 2017. The pool of 442 respondents includes a largely senior audience, with 69 percent holding positions at the GS/GM-12 level or above. 53 percent are supervisors with direct oversight of one or more employees, and 25 percent hold ranking positions in the Department of Defense. Respondents represent over 30 federal agencies and hold a variety of job functions, with highest input from project/program managers, technical/scientific personnel, and administrative staff.

1. KrebsOnSecurity: "Hacked Cameras, DVRs Powered Today's Massive Internet Outage." October 16, 2016.
2. White House: "Fact Sheet: National Cybersecurity Action Plan." February 9, 2016.
3. McKinsey&Company: "Internet of Things: Sizing Up the Opportunity." December 2014.
4. CSIS: "Leveraging the Internet of Things for a More Efficient and Effective Military." September 2015.

Executive Summary

Security is seen as a critical issue and top priority for IoT devices

When it comes to the devices and sensors their agency uses to transmit data, a high majority of respondents believe security (60%) takes top priority over other features like stability (17%), accuracy (13%), and speed (11%). 2 in 3 respondents say the ability to capture and share information from such devices is important, and 89% believe that securing these devices is essential to executing their mission. In spite of this, 58% say they are only somewhat, not very, or not at all confident in the security of their edge devices.

Slow procurement policies and insufficient funding complicate IoT security efforts

Even though 74% of respondents believe the IoT should be as tightly secured as core infrastructures, a host of challenges stand in the way. Limited funding to invest in IoT security (39%) and adherence to inadequate procurement processes (39%) lead the list of challenges. A shortage of technical expertise (30%), inability to adapt to new threats (23%), and lack of leadership buy-in (19%) further compound these difficulties, challenging agencies to innovate new security solutions that can keep pace with a constantly changing threat landscape. Currently, enforcing stringent password requirements, built-in encryption, and automated security patches are the most cited practices for securing edge data. However, nearly half of respondents (48%) don't know how their agency plans to secure its IoT in the near future, casting some doubt on the extent to which built-in encryption and automation actually feature in current security architectures.

Respondents support a standardized, government-led framework

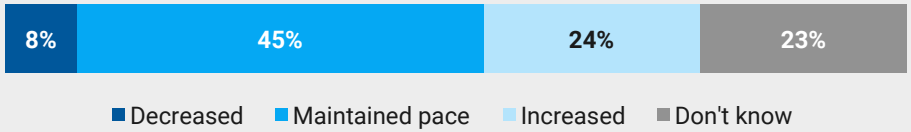
When asked how the IoT should be secured going forward, most respondents strongly support a government-driven framework that would enable shopping from among pre-approved security solutions offered by the commercial sector. Specifically, respondents support more rapid deployment of automated security patches, a standardized application program interface (API) enabling tailored security solutions, and the flexibility to use in-house solutions for most critical data while securing less sensitive data with commercial options. Even though the National Security Agency has devised the Commercial Solutions for Classified (CSfC) framework to address these needs, a high portion of respondents are unfamiliar with the program — a sign that more can be done to raise awareness of the initiative and others like it.

Research Findings

Respondents note steady, but continued gains in IoT investments at their organizations

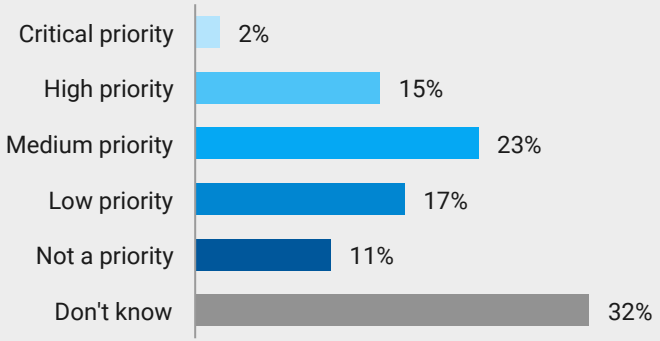
A plurality of respondents (45%) believe their agency has largely maintained pace from the previous year when it comes to expanding their network of IoT devices. In a sign of continued growth, three times as many respondents observed an increase to their network's edge (24%) as those who reported a scaling back (8%). In other words, while adoption efforts remain steady, the scale tilts toward growth.

In the past year, would you say your organization has increased adoption, decreased adoption, or maintained pace when it comes to expanding the use of Internet-enabled devices (IoT)?



Percentage of respondents, n=442
Note: Percentages may not add up to 100% due to rounding

To what extent is your organization prioritizing the expansion of Internet-enabled devices (IoT) (e.g., via sensors, cameras) over the next 12 months?



Percentage of respondents, n=439
Note: Percentages may not add up to 100% due to rounding

1 in 4

respondents say their organization has increased adoption of IoT devices and applications within the last year, indicative of the IoT's continuing growth and utility in public sector services.

57%

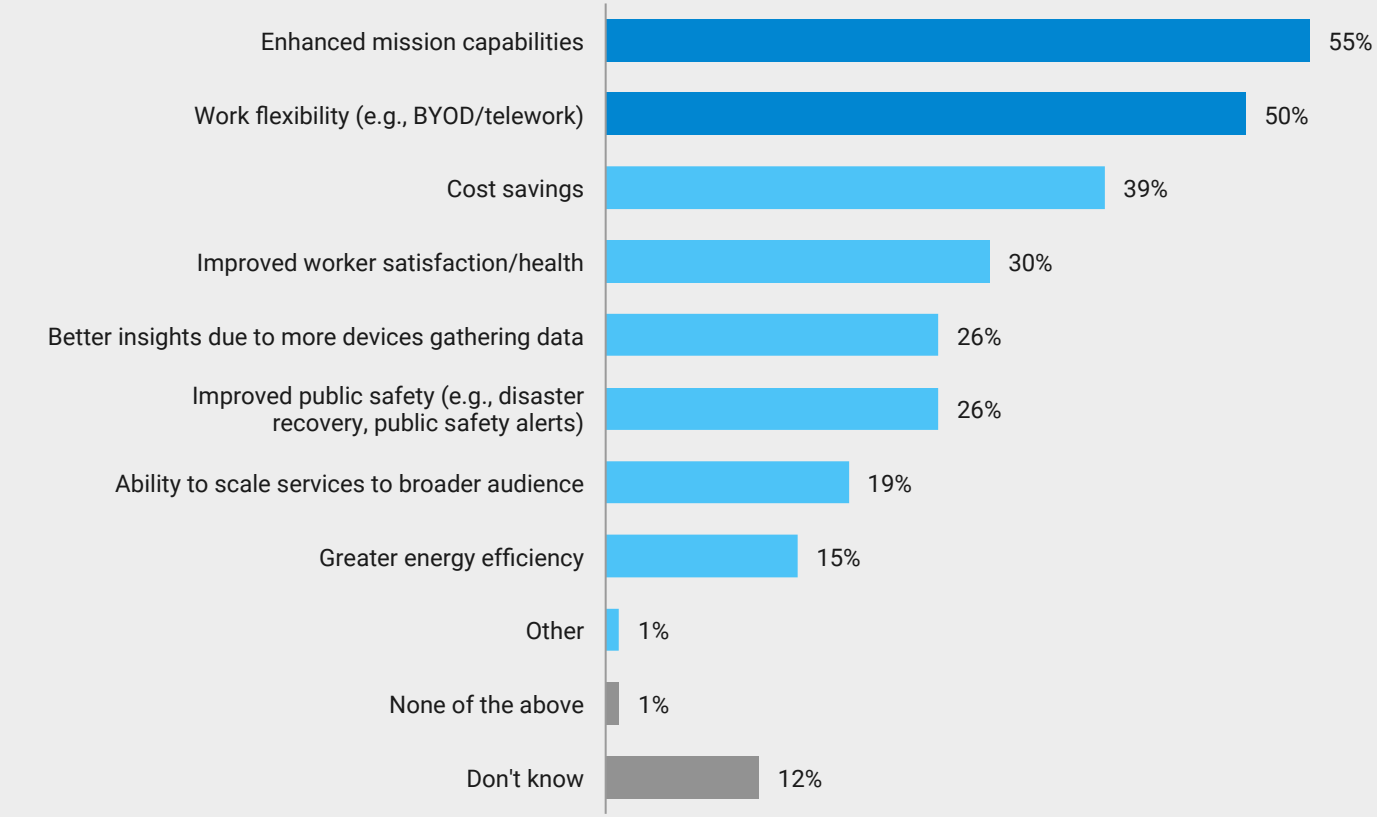
of respondents believe IoT expansion will merit at least some level of priority status for their agency in the year ahead, with 17% describing it as a critical or high priority.

From 2011 to 2015, the federal government spent nearly $35 billion in IoT investments, with 2015 alone seeing a 20% increase in IoT spending (at $8.8 billion) over the previous year.[5] While it is too early to tell how IoT's growth will be impacted by a changing administration, respondents anticipate continued investments to harnessing IoT technology at their agency.

5. Business Insider: "The US government is pouring money into the Internet of Things." May 31, 2016.

Enhanced mission capabilities, greater work flexibility, cost savings are leading catalysts for IoT growth

Leading Benefits to Expanding the IoT



Percentage of respondents, n-325
Respondents were asked to select all that apply

When asked which benefits were most responsible for driving IoT expansion at their agency, respondents point to enhanced mission capabilities (55%) and the ability to work flexibly from home or in remote locations (50%) as the top drivers. The portable nature of IoT devices grants federal employees more leeway and mobility to fulfill their mission beyond department walls in Washington. Another major draw is its massive cost saving potential. For example, by installing thousands of low-cost connected sensors in government buildings since 2012, the General Services Administration (GSA) estimates to have saved $15 million per year.[6]

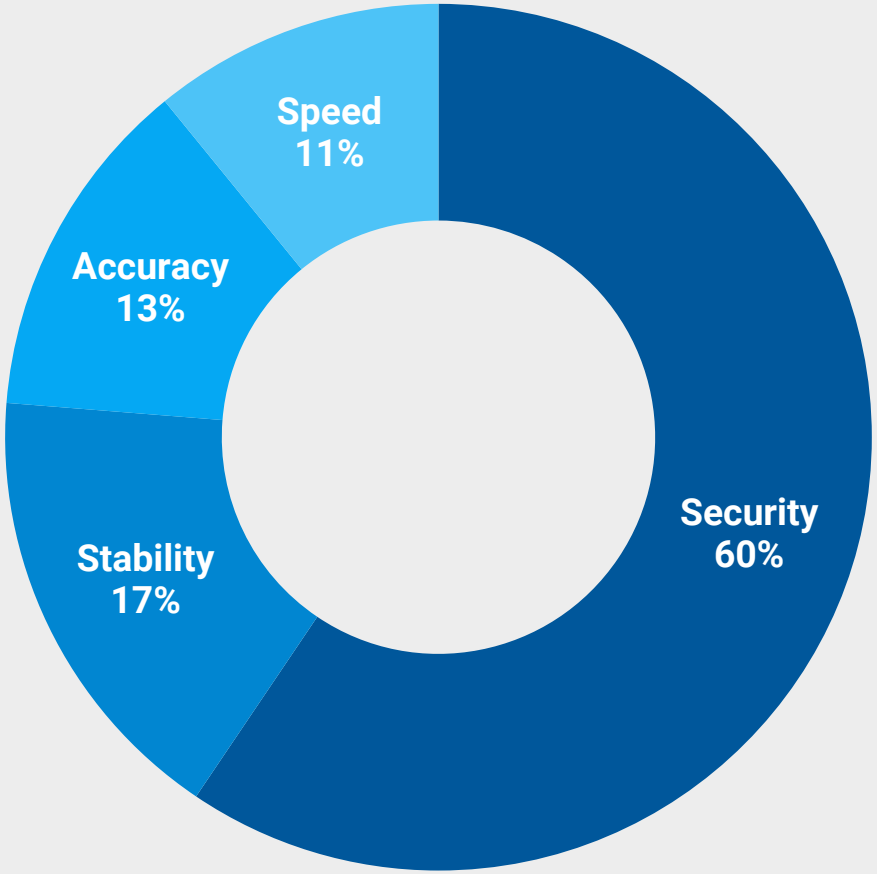
55%

of respondents cite enhanced mission capabilities as the benefit most responsible for driving IoT expansion at their agency.

6. Center for Data Innovation: "How is the Federal Government Using the Internet of Things?" July 25, 2016.

3 in 5 respondents say security is the top priority when developing devices for use in the field

When it comes to the devices and sensors your organization uses to transmit data, which performance feature do you feel is prioritized the most?

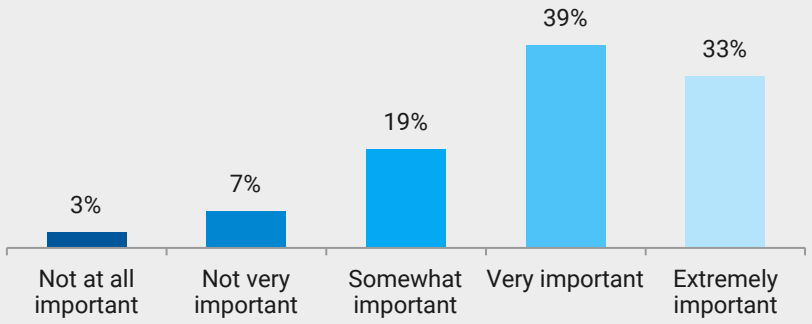


Percentage of all respondents, n=325
Note: Percentages may not add up to 100% due to rounding

> "There is a small—and rapidly closing window—to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.
>
> **Excerpt from NSTAC 2014 Report**
>
> The National Security Telecommunications Advisory Committee, qtd. in *Nextgov*: "Report: Government has only five years to secure the Internet of Things." November 2014.

More than half of respondents say ensuring security of data-sharing devices is 'extremely important'

When it comes to fulfilling your agency's mission, how important is capturing and sharing information from devices used in the field or at remote locations?

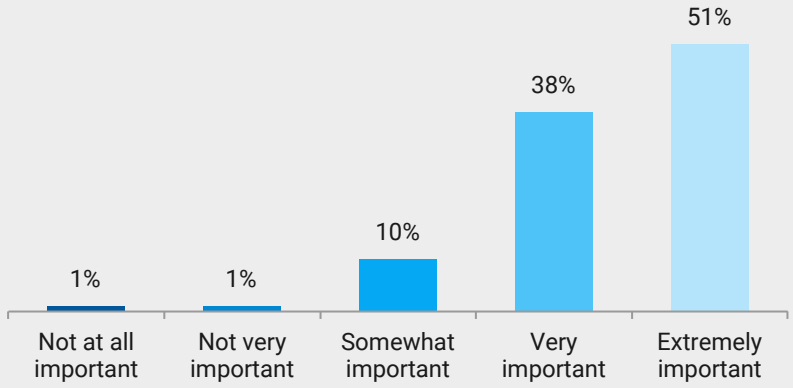


Percentage of respondents, n=299
Note: Percentages may not add up to 100% due to rounding

72%

of respondents believe the capability to capture and share information with IoT devices in the field to be very or extremely important to their agency's mission.

How important is it that the devices used to share such information are secure when operating at the edge?



Percentage of respondents, n=311
Note: Percentages may not add up to 100% due to rounding

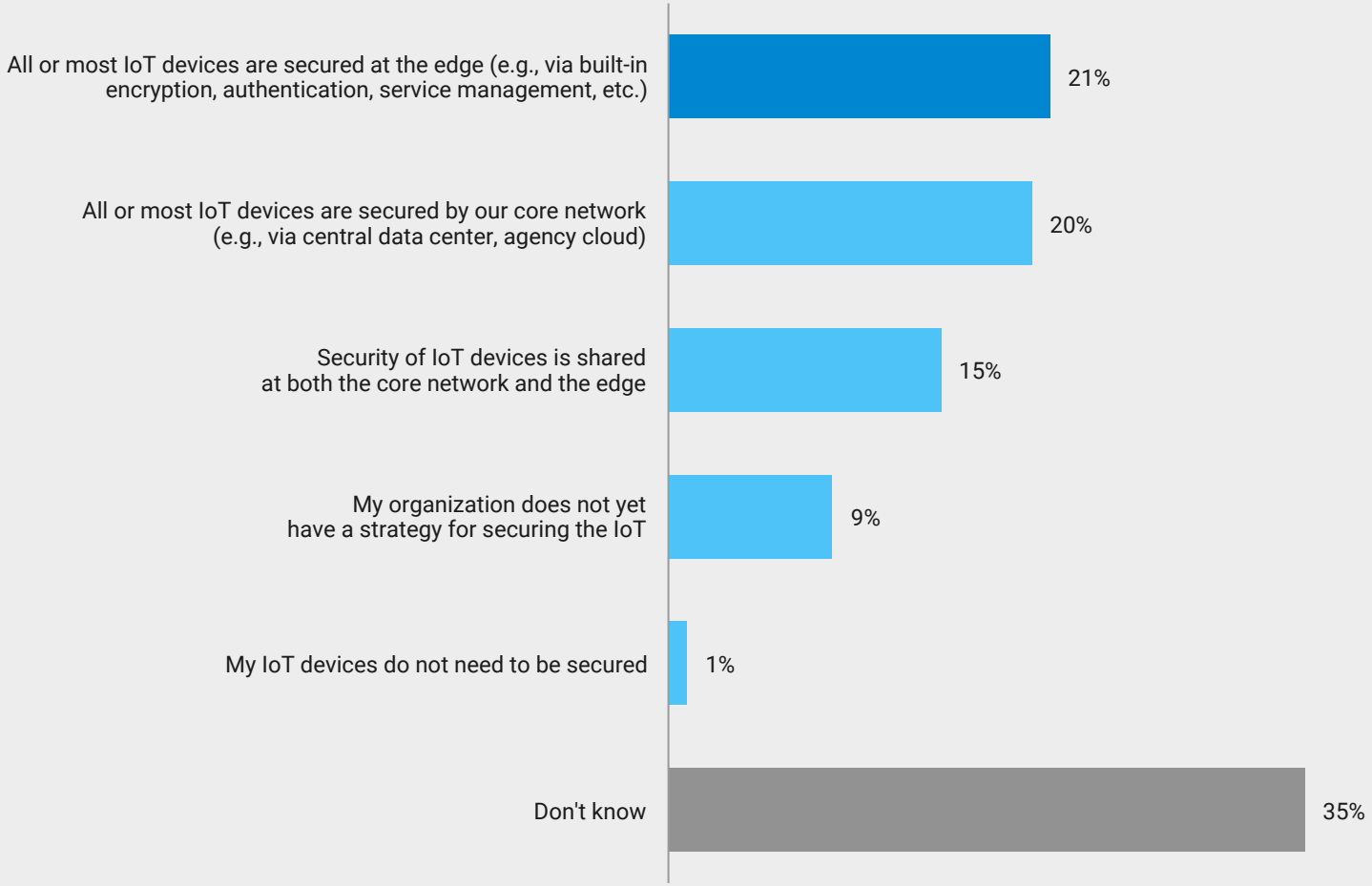
89%

of respondents express it is very or extremely important that such devices operating at the edge are secure from malicious attackers.

Current IoT security methods span the board, but are primarily split between edge and core

When asked how their organization currently secures its IoT, respondents appear split among a variety of approaches. 21% say they secure all or most devices through edge security protocols, like built-in encryption, authentication, and service management tools. On the other hand, 20% say they secure most of their devices through their core network, relying on central data centers and the cloud for protection.

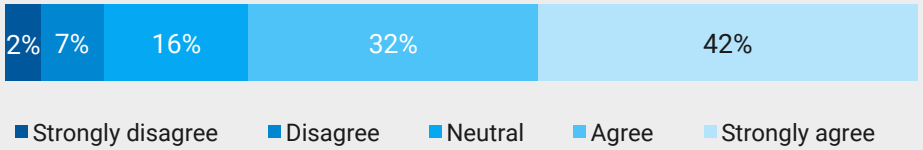
Which of the following best describes your organization's current method to secure its IoT?



Percentage of respondents, n=347
Note: Percentages may not add up to 100% due to rounding

The IoT should be accountable to baseline standards and secure as core infrastructures

"The federal government should set common minimum standards governing IoT security, rather than allowing each department/agency to set its own."

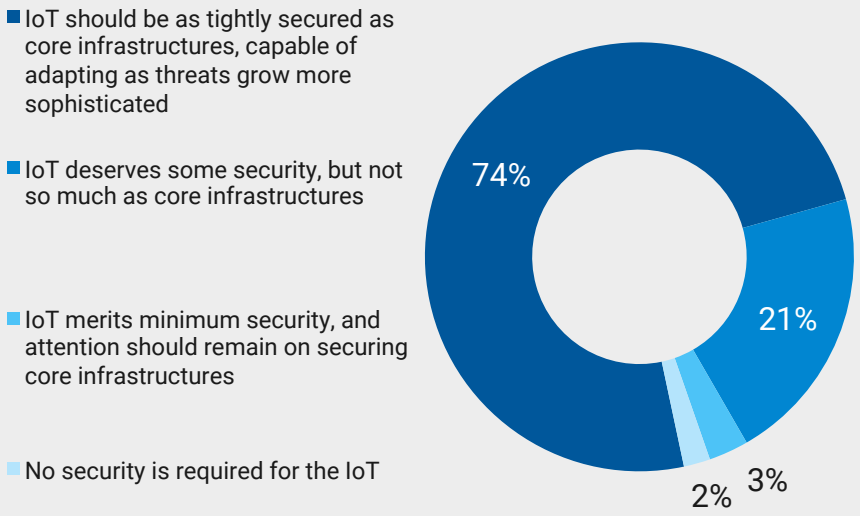


Percentage of respondents, n=298
Note: Percentages may not add up to 100% due to rounding

3 in 4

respondents agree or strongly agree that the government should set baseline standards governing IoT security, as opposed to relegating this governance to individual departments and agencies.

What degree of security do you feel is necessary in order to safeguard your organization's IoT?



Percentage of respondents, n=343
Note: Percentages may not add up to 100% due to rounding

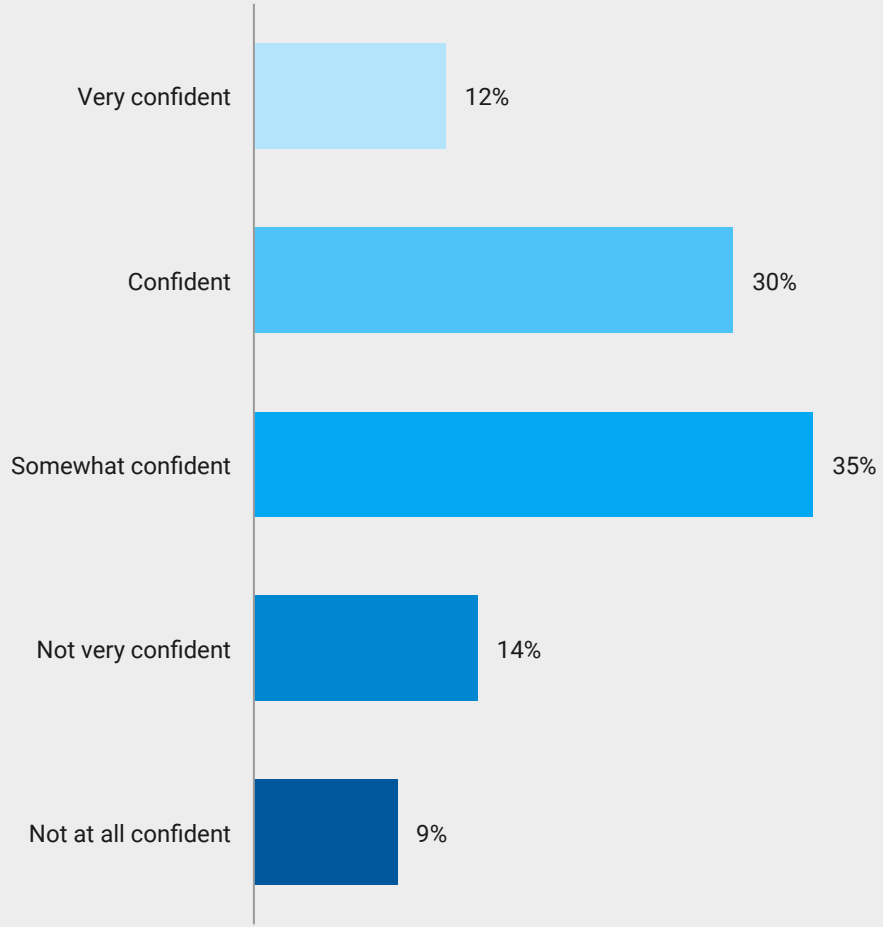
74%

of respondents believe the IoT should be as tightly secured as core infrastructures, like data centers and core servers, to keep pace with more sophisticated threats.

21% agree it deserves security, but not so much as that afforded to core infrastructures.

Respondents give mixed ratings to security of devices at the edge, with 1 in 4 showing low confidence

How confident are you that the devices your organization provides for use at the "edge" are secure (i.e., any physical location where such devices operate)?



Percentage of all respondents, n=379
Note: Percentages may not add up to 100% due to rounding

58%

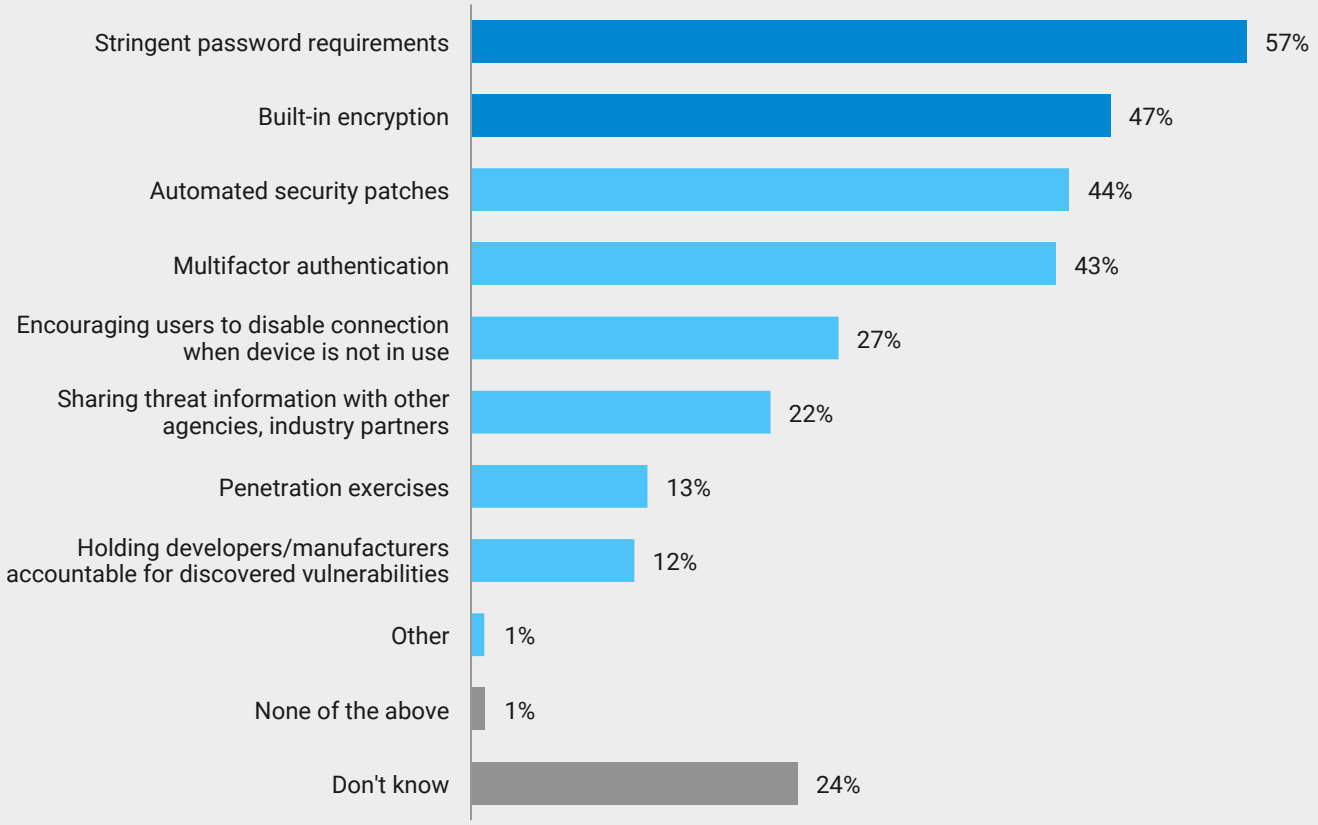
of respondents say they are only somewhat, not very, or not at all confident in the security of their edge devices.

"The benefits and risks of the IoT are evolving very quickly. These questions tend toward "single point-in-time" solutions, rather than a constantly evolving interaction with opportunities and threats. For the next decade or so, this will be a very fluid game like soccer or rugby, not baseball or football.

Survey Respondent

A range of security protocols are used, but 1 in 4 respondents are unsure how their agency secures IoT

To the best of your knowledge, which of the following methods does your organization currently use to secure devices at the edge?



Percentage of respondents, n=301
Respondents were asked to select all that apply

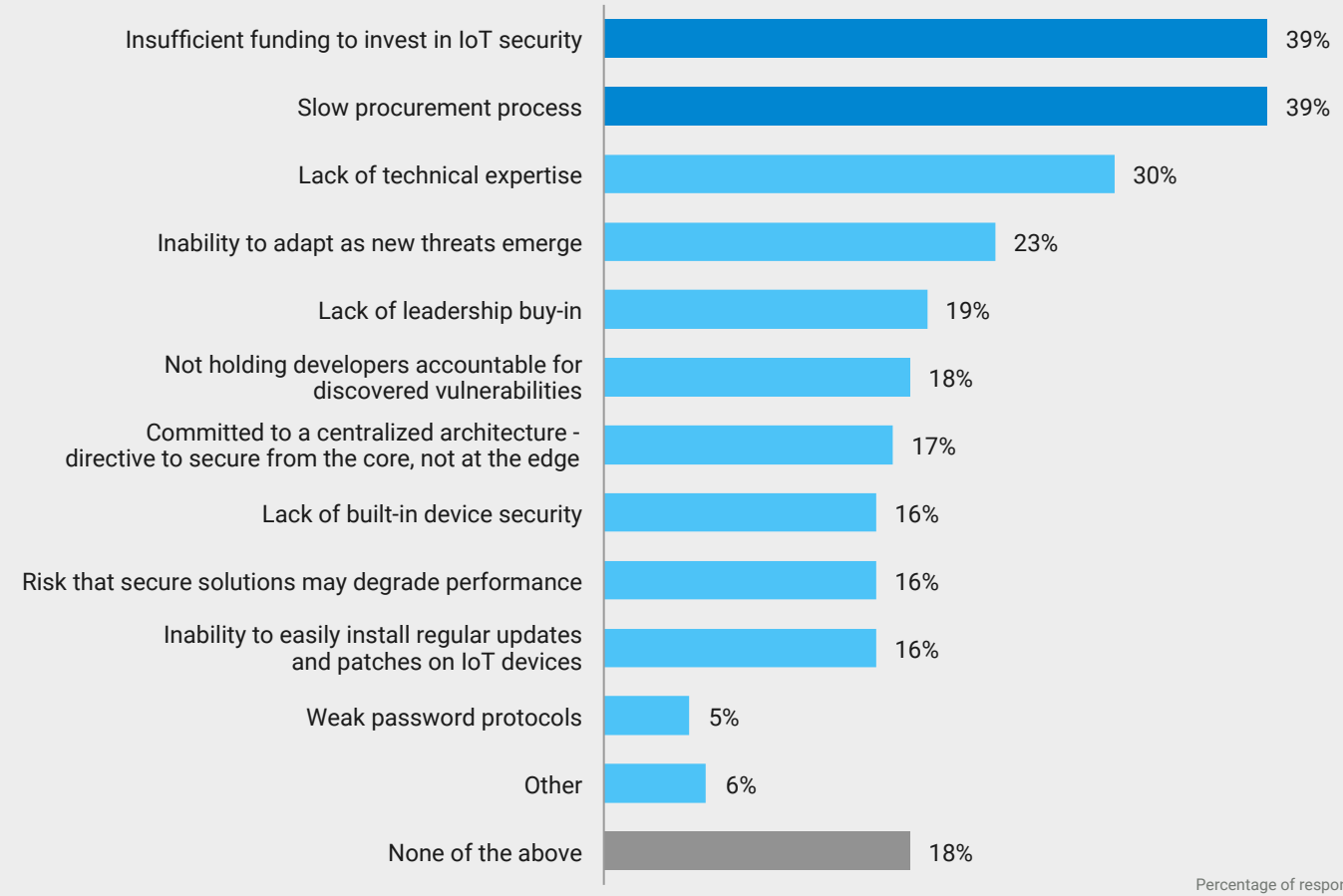
When it comes to ensuring security of devices at the edge, most respondents say their agency practices stringent password requirements (57%), built-in encryption (47%), and automated security patches (44%). Encryption, automated patches, and device authentication are good practices, but communicating cyber hygiene and accountability in the workplace is also essential. Currently, only 27% say their agency encourages users to disable connections when devices aren't in use, and just 12% say developers and manufacturers are held accountable for vulnerabilities discovered post-deployment.

1 in 4

respondents are unaware what methods their agency uses to secure IoT devices.

Slow procurement, insufficient funds, and lack of tech expertise are top barriers to IoT security

Leading Challenges to Edge Security



Percentage of respondents, n-373
Respondents were asked to select all that apply

Insufficient funding (39%), slow procurement processes (39%), and a shortage of technical expertise (30%) are the most cited impediments to improving IoT security at the network's edge. While the White House aims to funnel more than $19 billion into cybersecurity for fiscal year 2017, it is not yet clear how much of this will be devoted specifically to enhancing security of IoT technology.[7]

39%

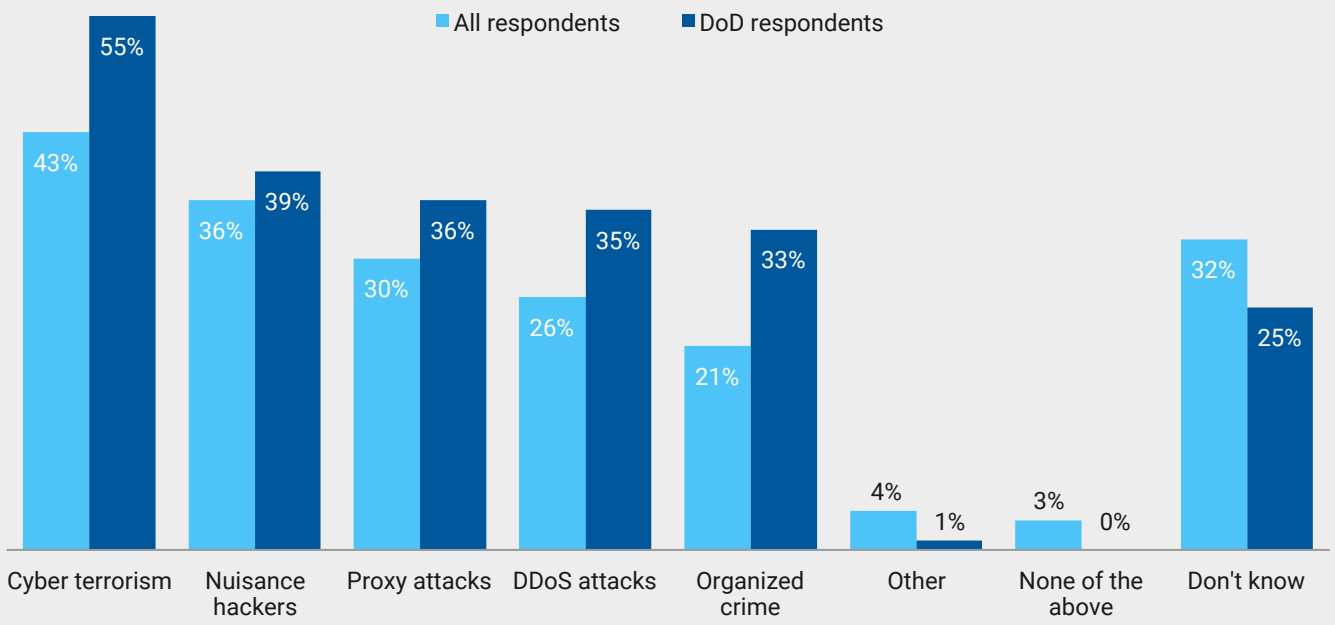
of respondents cite slow procurement processes as a leading barrier to improving their edge security.

7. White House: "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016.

Cyber terrorism leads list of perceived threats to IoT networks

When asked to identify which threats to the IoT concerns their organization the most, 43% of all respondents say cyber terrorism is the leading threat given its capacity to compromise sensors controlling nuclear power plants and other critical infrastructures.

When it comes to securing your agency's network of devices, which of the following threat vectors concerns your organization the most?



Percentage of respondents, n=294 and n=70
Respondents were asked to select all that apply

Attacks by nuisance hackers (36%) on residential IoT devices (e.g., unprotected webcams, home systems, medical sensors) are also poised to grow in scale and sophistication. Proxy attacks (30%) and distributed denial of service (DDoS) disruptions (30%) will take advantage of the decentralized nature of the IoT by exploiting local vulnerabilities, redirecting user queries through copy-cat search engines, or flooding an online service with traffic from multiple systems.

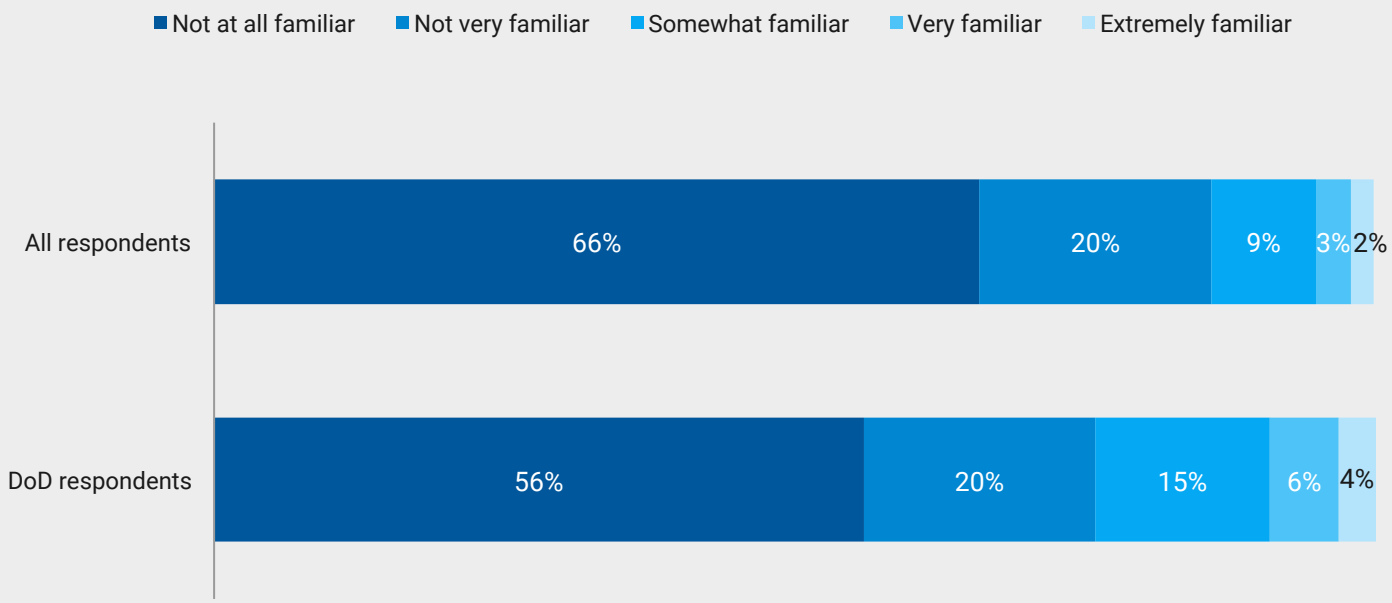
1 in 3

respondents are unable to say what threats to the IoT give their organization the most concern.

2 in 3 respondents have never heard of NSA's Commercial Solutions for Classified (CSfC) program

66% of all respondents say they have no prior familiarity with the Commercial Solutions for Classified (CSfC) program.[8] A creation of the National Security Agency, CSfC was designed several years ago after leaders recognized that traditional procurement was unable to keep pace with changing mission objectives and evolving user needs.

How familiar are you with the Commercial Solutions for Classified (CSfC) program?



Percentage of respondents, n=323 and 82, respectively
Note: Percentages may not add up to 100% due to rounding

Instead of gathering requirements and contracting a vendor to produce a unique product, CSfC provides a set of baseline security requirements that allow the development of packages which are turnkey commercial solutions for agencies.

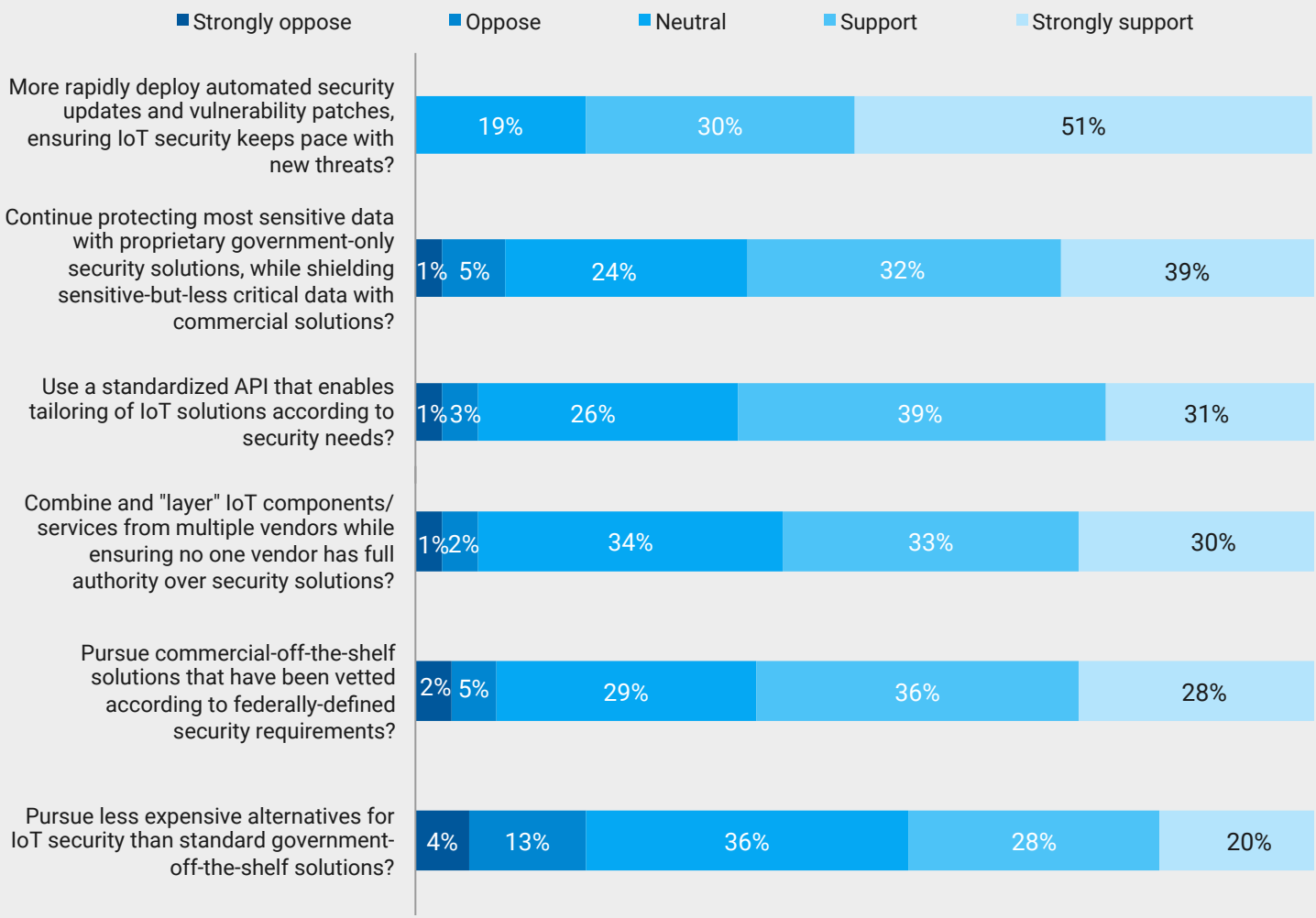
86%
of all respondents say they are not very or not at all familiar with the CSfC program.

8. National Security Agency: Commercial Solutions for Classified (CSfC) Program. Link

Despite low awareness of the framework, respondents strongly support basic tenets of CSfC

The following graphic depicts respondents' level of support for various components licensed under a standardized, government-led framework. Respondents were not informed that all components listed actually correspond to existing practices in the CSfC framework.

As a step toward expediting the IoT security assurance timeline, to what degree do you support the development of a standardized, government-led framework that would allow agencies to…



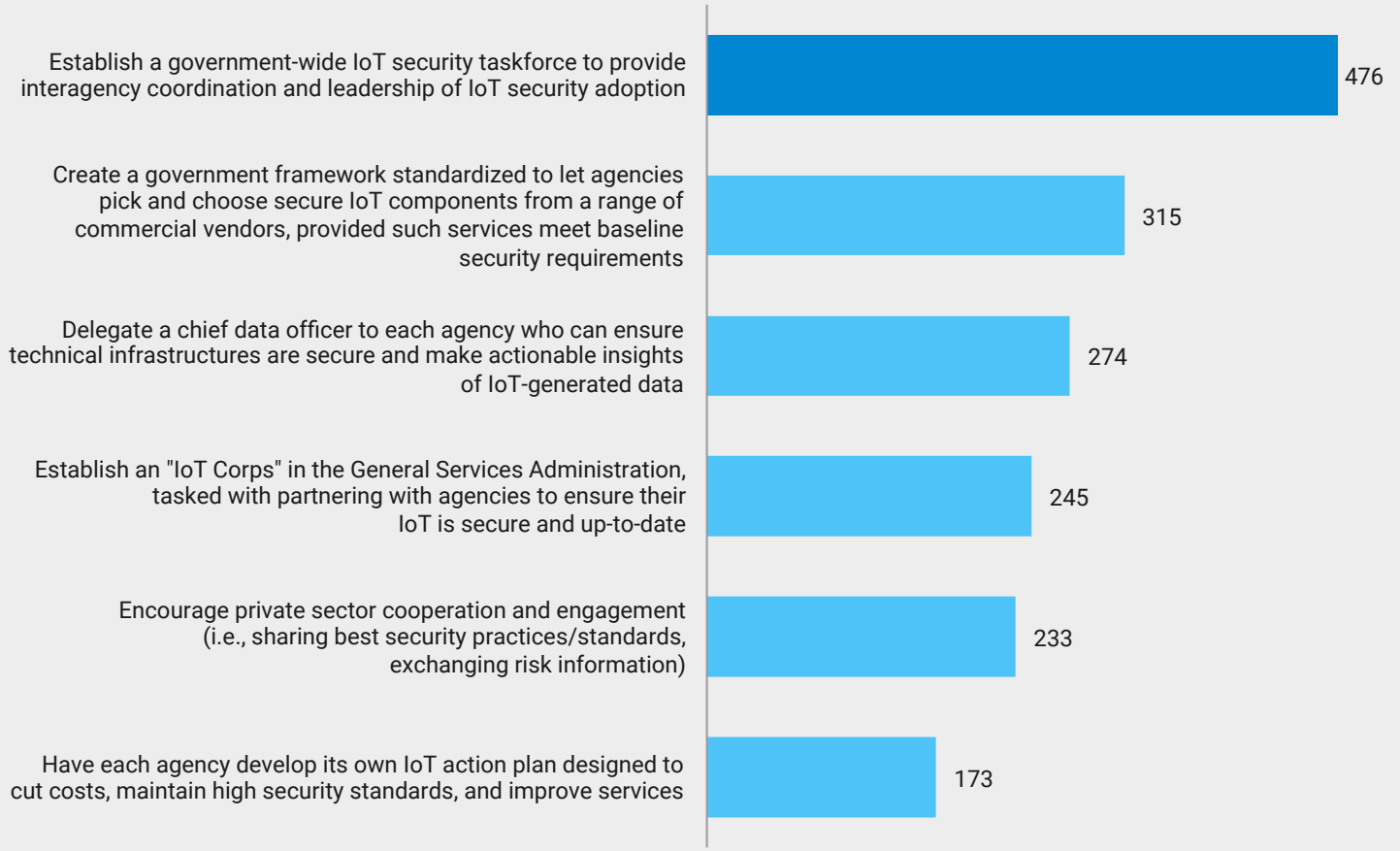
Percentage of respondents, n varies=283-289
Note: Percentages may not add up to 100% due to rounding

When it comes to securing IoT, respondents prize government-wide coordination and leadership

Respondents were asked to rank their top 3 choices among the following series of proposals, which are taken from a 2016 report on federal IoT security authored by the Center For Data Innovation.[9]

Proposals for Securing the IoT

Ranked by respondents according to perceived effectiveness



Ranked by Borda count, n=286

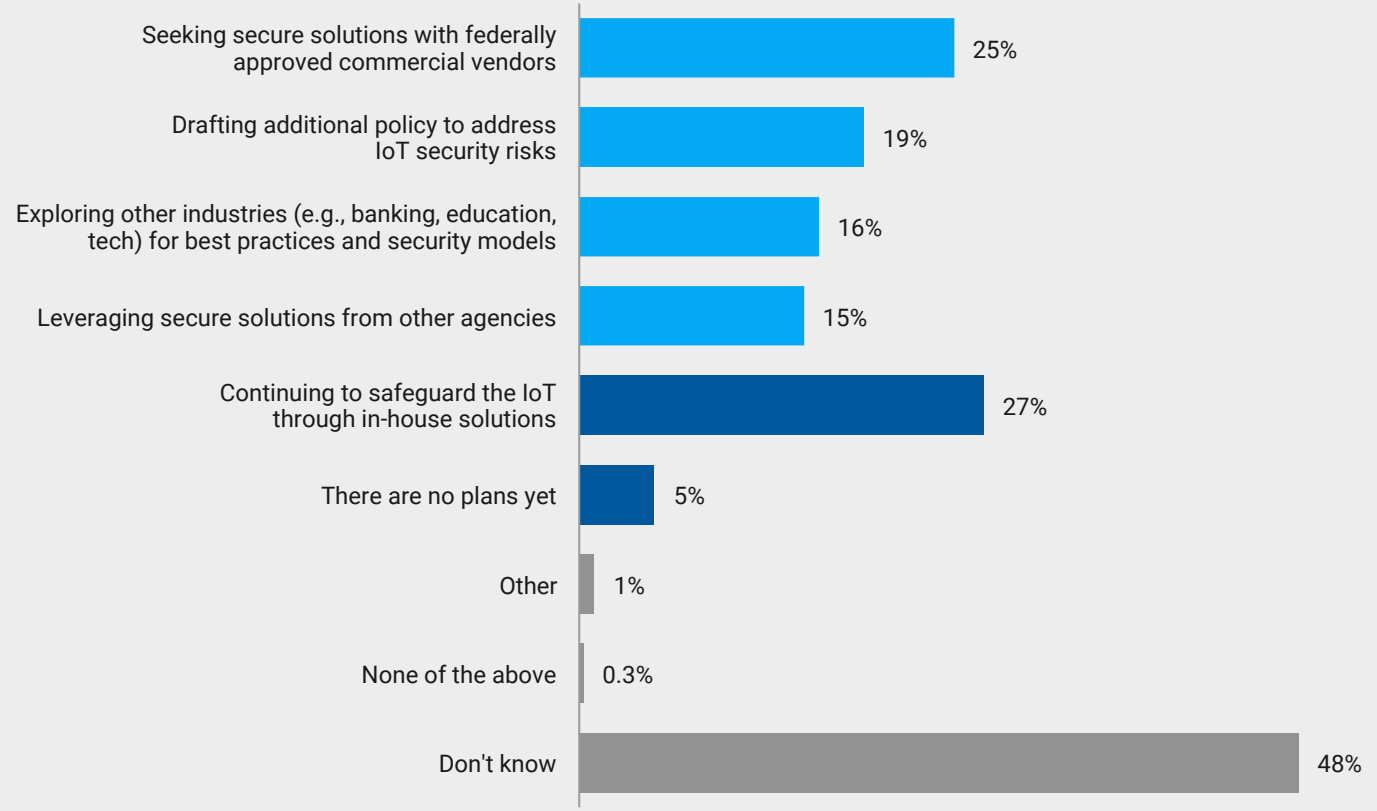
Respondents were asked: "The following are a series of proposals aimed at promoting more secure adoption of IoT. Please rank the top three choices you feel would be most effective."

Rankings and total scores are displayed here using the Borda count method, where each answer choice earns points based on the order in which respondents placed them. Each respondent's top answer choice receives the maximum score of n points for that respondent, where n is equal to the total number of options. Each subsequent choice receives 1 less point than the one ranked ahead of it. Unranked answer choices receive zero points. Please see Appendix for further detail.

9. Center for Data Innovation: "How is the Federal Government Using the Internet of Things?" July 25, 2016

Respondents show growing interest in addressing IoT security risks beyond current in-house solutions

Going forward, which of the following best describes your organization's plan for securing its IoT?



Percentage of respondents, n=295
Respondents were asked to select all that apply

When asked to identify how their agency plans to secure its IoT in the near future, 27% of respondents say they will continue to use in-house solutions, edging out those with plans to pursue federally-approved commercial solutions (25%). Nearly 1 in 5 anticipate drafting additional policy to address outstanding IoT security risks, with some indicating they will seek cues from other industries (16%) or leverage existing solutions from neighboring agencies (15%). Almost half (48%) are uninformed when it comes to their agency's IoT security strategy for the near future.

48%

of respondents are unsure how their agency plans to secure the IoT in the near future.

Final Considerations

When considering how to secure data at the tactical edge:

—

Prioritize security upfront

The IoT's rapid growth demands that agencies invest upfront in security. While it may be expedient to bolt on security for devices already in use, this is neither sustainable nor cost-efficient in the long term. Instead, agencies should prioritize security at the earliest stages of development, communicating basic IoT threat awareness to employees and investing in encryption and automation.

Some agencies are already making good progress in this effort. In recent months, the Department of Homeland Security and Department of Commerce have released strategic action plans for securing the IoT, with developer accountability, cyber hygiene, encryption, and automated updates drawing special attention. [10,11]

—

Harness private sector innovation

As the data shows, respondents strongly favor a coordinated effort to standardize IoT security policy that allows freedom and flexibility when harnessing the latest commercial innovations. Certainly agencies can and should continue protecting most classified data with in-house solutions, but respondents see value in a framework that enables tailored, private sector packages to safeguard less sensitive data as well (71%).

—

Pursue government-led security initiatives

Government programs like NSA's CSfC are a positive step in this direction, providing agencies a multitude of options to build their IoT security architecture as they see fit, with the added assurance that such solutions have passed NSA's security benchmark.[12]

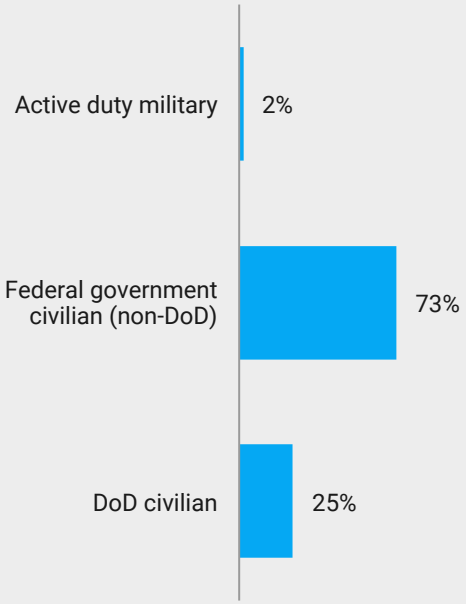
By sharing threat information with other departments and advocating government-led initiatives that leverage the latest in private sector innovations, federal agencies will be far better able to detect and defend against threats at the edge.

10. Department of Homeland Security: "Strategic Principles for Securing the Internet of Things." November 15, 2016.
11. Department of Commerce: "Fostering the Advancement of the Internet of Things." January 2017
12. National Security Agency: Commercial Solutions for Classified (CSfC) Program. Link

Respondent Profile

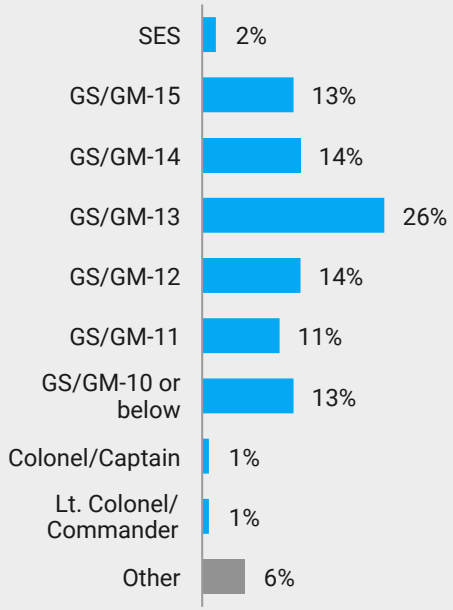
A majority of respondents are senior federal leaders within their organization

Employment Situation



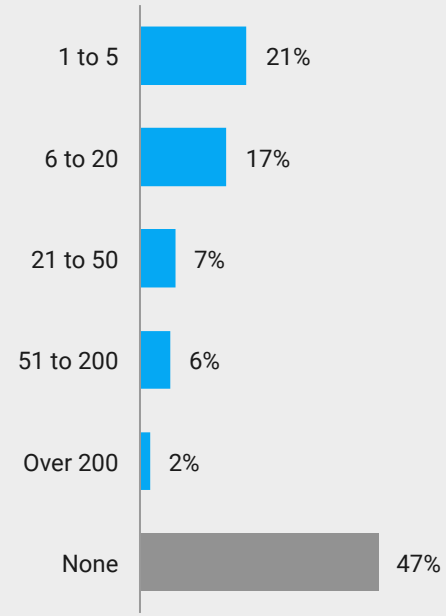
Percentage of respondents, n=412
Note: Percentages may not add up to 100% due to rounding

Grade/Rank



Percentage of respondents, n=284
Note: Percentages may not add up to 100% due to rounding

Reports/Oversees



Percentage of respondents, n=283
Note: Percentages may not add up to 100% due to rounding

1 in 4

respondents hold positions in the Department of Defense.

69%

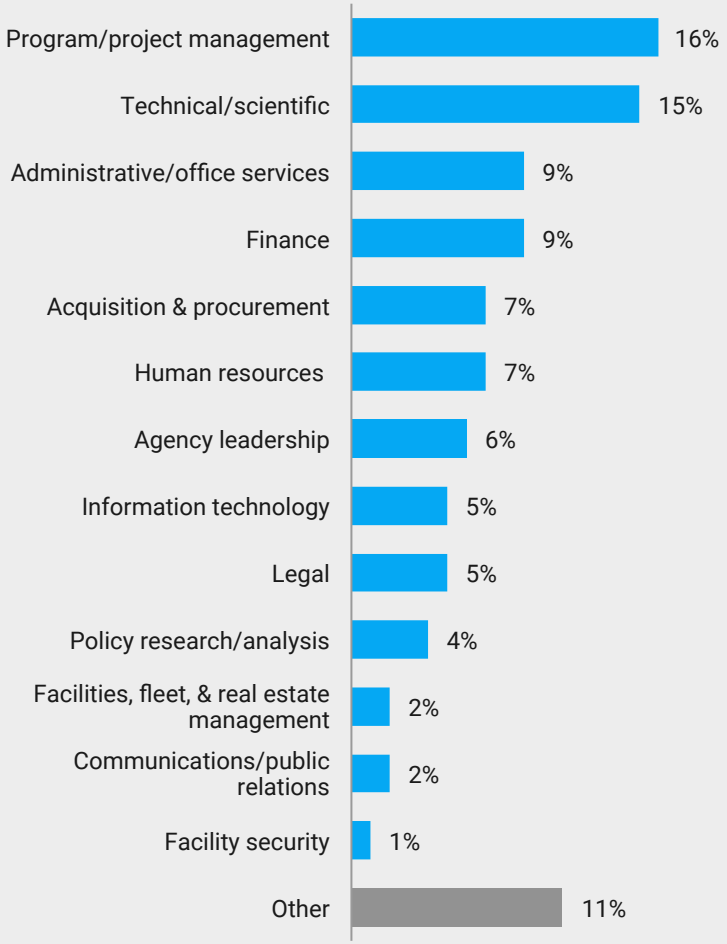
of respondents identify as working at the GS/GM-12 level or above, which includes members of the Senior Executive Service.

53%

of respondents are supervisors who oversee at least one employee either directly or through indirect reports.

Most widely represented are program managers, technical specialists

Job function



Percentage of respondents, n=283
Note: Percentages may not add up to 100% due to rounding

Respondents were asked to choose which single response best describes their primary job function. "Other" includes law enforcement, resource management, and policy integration.

Departments and agencies represented

- Treasury
- Army
- Veterans Affairs
- Office of the Secretary of Defense
- Homeland Security
- Interior
- Agriculture
- Air Force
- Navy
- General Services Administration
- Health & Human Services
- Social Security Administration
- Environmental Protection Agency
- Justice
- Energy
- National Aeronautics & Space Administration
- Commerce
- State
- Multiple Departments/ Agencies (e.g., IPO)
- Government Accountability Office
- Agency for International Development
- Combatant Commands
- Education
- Housing & Urban Development
- Labor
- Central Intelligence Agency
- Congress/Legislative Branch
- Joint Chiefs of Staff
- Marine Corps
- National Science Foundation
- Small Business Administration
- Transportation
- Other independent agency

Respondents, n=405

Departments and agencies are listed in order of frequency.

Appendix

The following graphic explains Borda count methodology for the question on Page 17, which asked respondents to rank their top three choices (among six possible proposals) they perceive as the most effective ways to secure the IoT going forward.

The following are a series of proposals aimed at promoting more secure adoption of the IoT. Among the choices presented, please rank the top three you feel would be most effective.

	Count per rank						Total	Borda count
	1	2	3	4	5	6		
Establish a government-wide IoT security taskforce to provide interagency coordination and leadership of IoT security adoption	101	61	51	0	0	0	213	476
Create a government framework standardized to let agencies pick and choose secure IoT components from a range of commercial vendors, provided such services meet baseline security requirements	51	60	42	0	0	0	153	315
Delegate a chief data officer to each agency who can ensure technical infrastructures are secure and make actionable insights of IoT-generated data	48	39	52	0	0	0	139	274
Establish an "IoT Corps" in the General Services Administration, tasked with partnering with agencies to ensure their IoT is secure and up-to-date	32	51	47	0	0	0	130	245
Encourage private sector cooperation and engagement (i.e., sharing best security practices/standards, exchanging risk information)	24	49	63	0	0	0	136	233
Have each agency develop its own IoT action plan designed to cut costs, maintain high security standards, and improve services	30	26	31	0	0	0	87	173
Number of respondents	286	286	286	0	0	0	-	-

Ranked by Borda count, n=286

Rankings and total scores are displayed here using the Borda count method, where each answer choice earns points based on the order in which respondents placed them. For instance, if a respondent's ranked choices were 1) "establish a government-wide IoT taskforce…", 2) "create a government framework…", and 3) "delegate a chief data officer…", those responses would receive 3, 2, and 1 points respectively. These points would be added to the Borda count of each answer choice.

With 286 respondents and 3 ranking slots available, the maximum score possible for any single answer choice (i.e., if every respondent ranked it as their top outcome) is equal to 858 points (286 x 3).

About

Government Business Council

Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Report Author: Daniel Thomas

Contact

Nicholas McClusky
Director, Research & Strategic Insights
Government Business Council
Tel: 202.266.7841
Email: nmcclusky@govexec.com

govexec.com/insights
@GovExecInsights

Brocade Communications Systems, Inc.

Brocade® networking solutions empower federal agencies to achieve their critical initiatives in a world where applications and information reside anywhere. By delivering open, secure, software-driven, and hardware-optimized solutions, Brocade helps the government to modernize their IT networks. Learn more about best-in-class networking solutions at www.brocade.com.

Contact

Ginger Kessler
Director, Federal Marketing
Brocade
Tel: 301.512.6843
Email: gkessler@brocade.com