2017 Global Information Security Workforce Study

U.S. Federal Government Results

(ISC)²®

CENTER FOR CYBER SAFETY AND EDUCATION

Booz | Allen | Hamilton

Study Objectives

To **obtain feedback** regarding certification, training and educational requirements for organizations and professional development

To **identify trends** and issues related to information security from both members and non-member security professionals

To **understand potential gaps** in organizational security

To **forecast** what positions will be most highly sought after in the next 3 to 5 years

Research Background

8th GISWS, Bi-annual study, first one released in 2004

In partnership with **Frost & Sullivan**, **Booz Allen Hamilton** and **Alta Associates**

Likely the **largest study of the information security profession** ever conducted

Of the over **19,600** - ~12,300 were (ISC)^2 members and ~7,300 were non-members

Conducted using an on-line web based survey using the (ISC)^2 membership list, Invitations via email

Fieldwork: June 2016 – September 2016

Sample Structure

Sample	U.S. Federal Government
2,620	Total
1,614	Military (Federal DoD personnel including both contractors/non-contractors)
1,006	Non-military (Federal civilian personnel including both contractors/non-contractors)

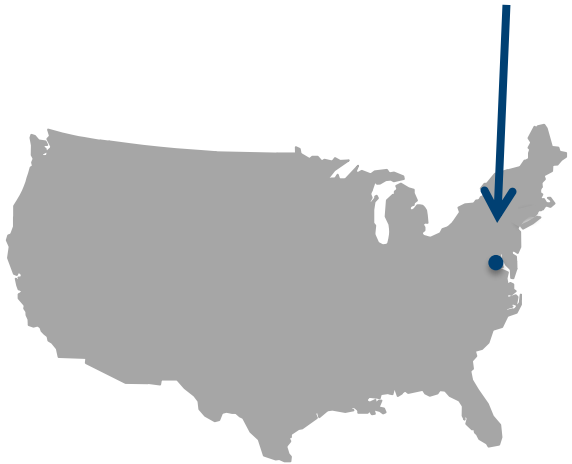
Respondent Profile

85% 15%

Average age: 47

40% have bachelor's degree
(or equivalent)
49% have master's or PhD
(or equivalent)

44% reside in
the DC Metro area*



*DC Metropolitan area – Maryland, Virginia, Washington D.C.

Respondent Profile (Cont.)

Top three job position listing:
17% information assurance manager
13% security analyst
11% security engineer

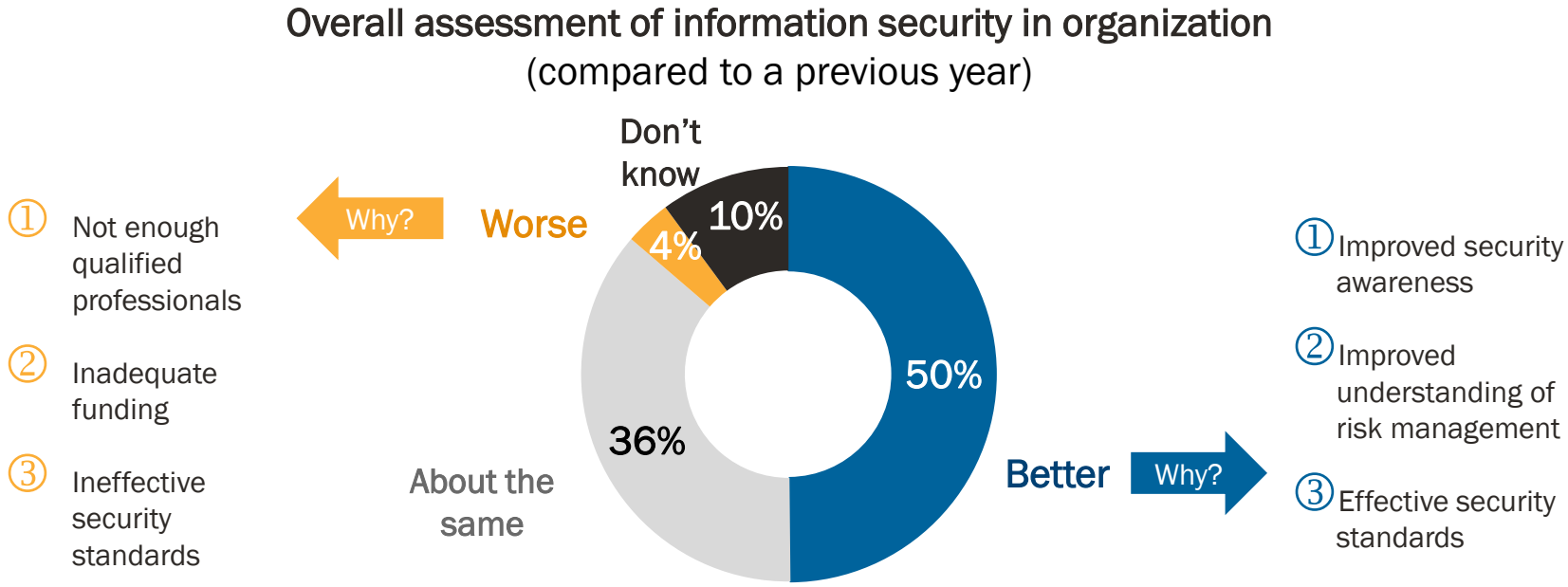
On average **15 years** of experience

47% are ex-military / military veterans

Average salary: **$118,000**

Assessment of U.S. Government Information Security

Half respondents say government security has improved

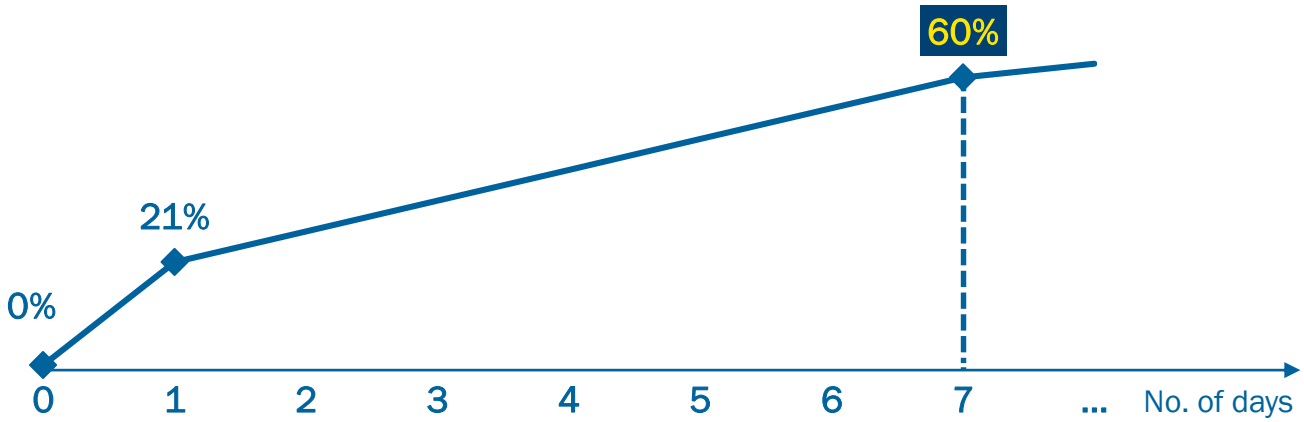


Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N=2620, Q33A: Overall, is your organization's information security better or worse off than a year ago?; N (2017, better off)=1306, N (2017, worse off)=94, Q33B/C: Why do you say that your organization's security is better/ worse off than a year ago?

Threat Response

Over half respondents (60%) say remediation would take up to a week

Time needed to remediate the damage in case of a targeted attack

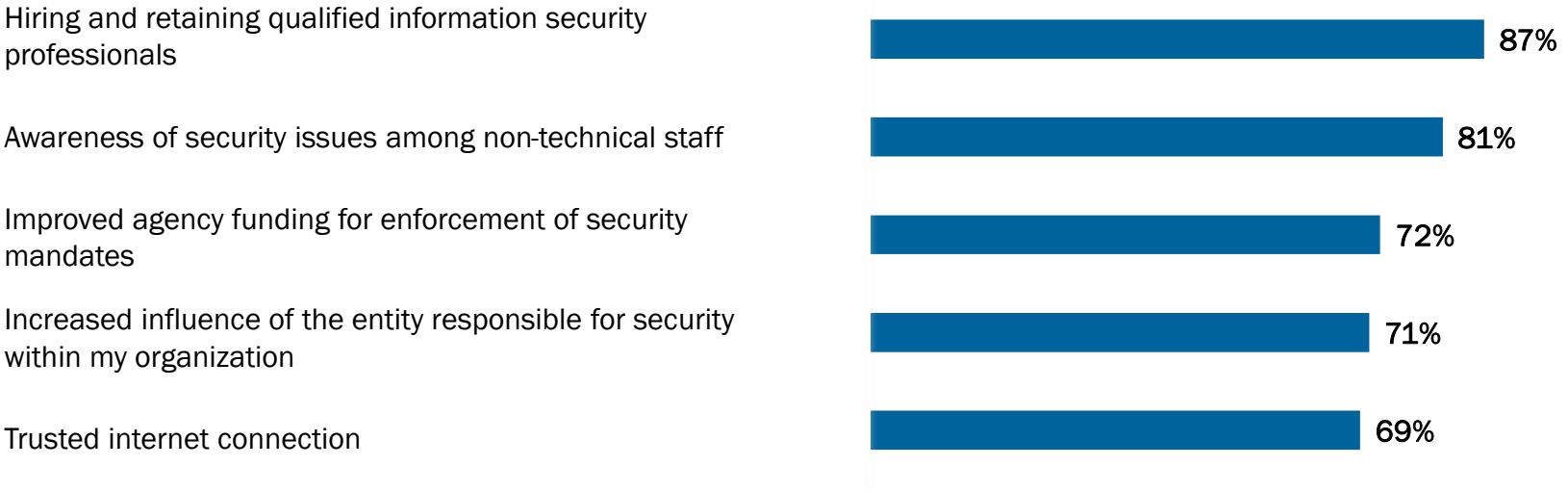


20% of respondents are unable to assess the time

Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620, Q31C: If your organization's systems or data were compromised by a targeted attack, how quickly do you predict it would take to remediate the damage?

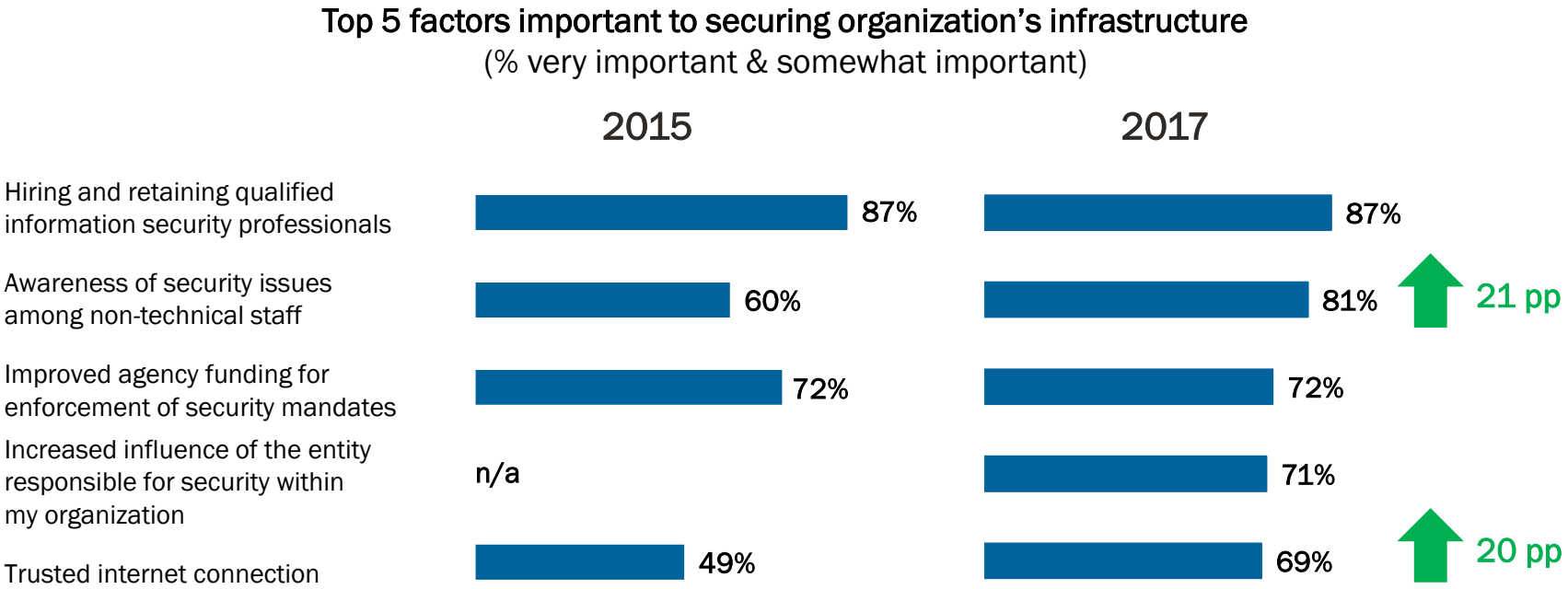
Top 5 factors important to securing organization's infrastructure

(% very important & somewhat important)



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2258
G2: How would you rate the importance of each of the following in effectively securing your organization's infrastructure? – Top two box scores

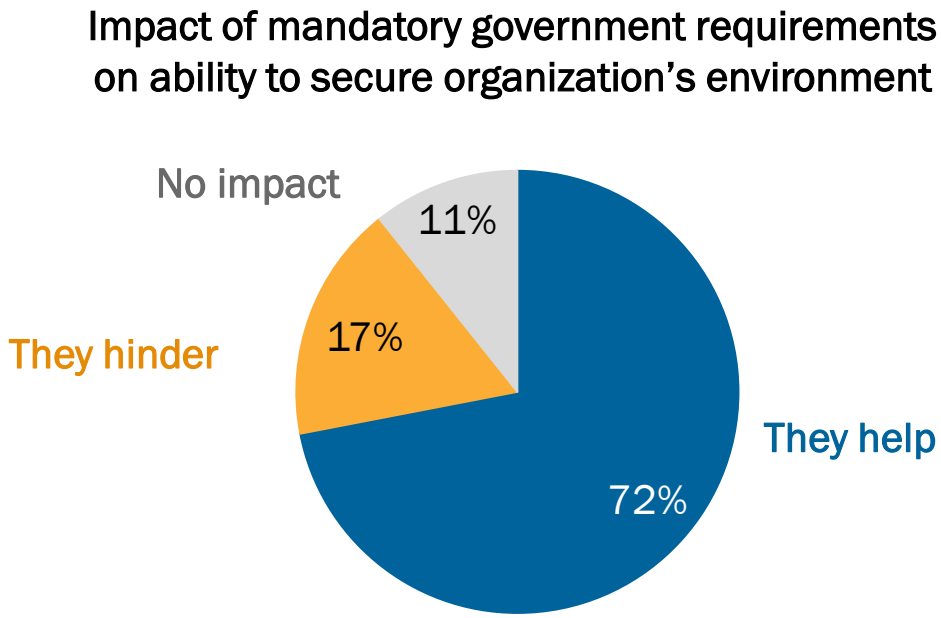
Increased importance: security awareness and TIC



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2258, N (2015)=1059
G2: How would you rate the importance of each of the following in effectively securing your organization's infrastructure? – Top two box scores

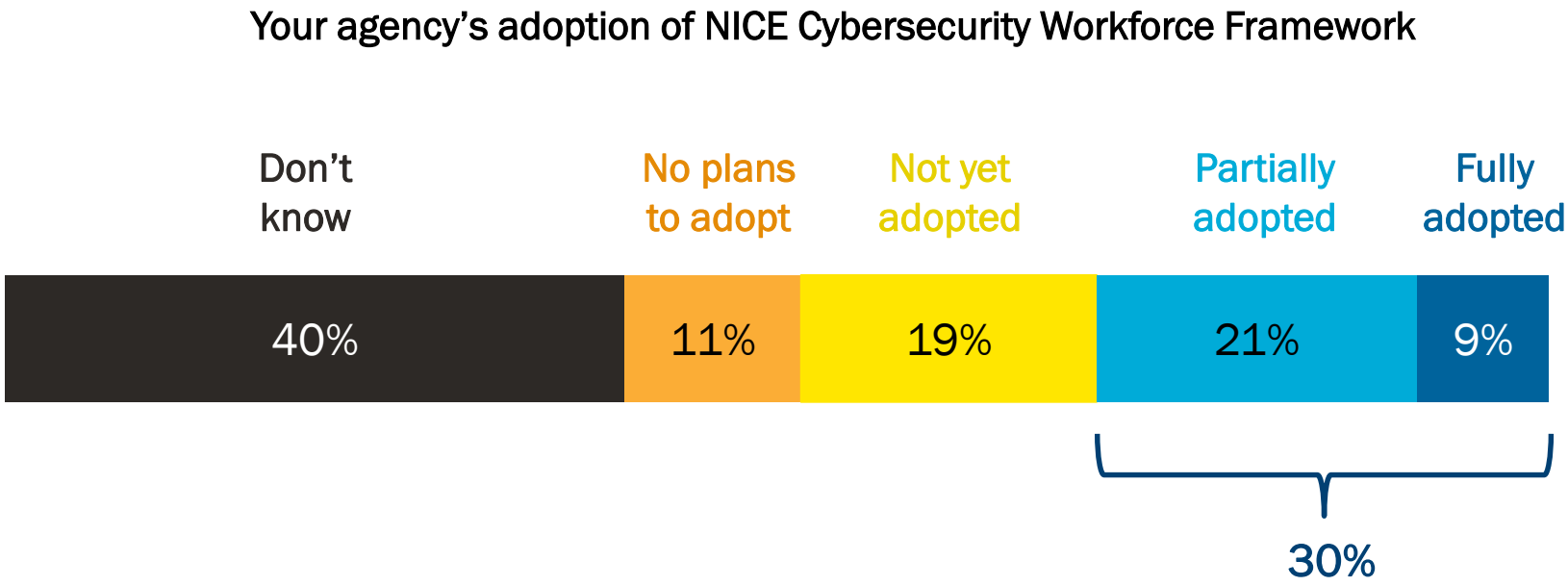
Government's Requirements & Legislation

72% of respondents say mandatory requirements help



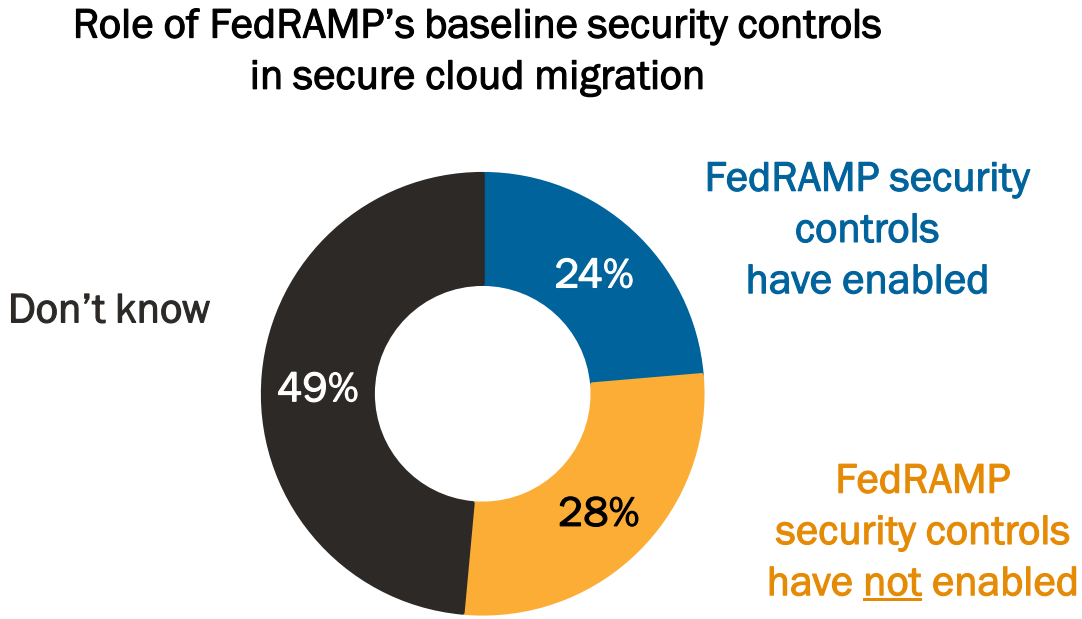
Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2258
G3: How do mandatory government requirements impact your ability to secure your environment?

30% of respondents claim their organizations have at least partially adopted NICE Cybersecurity Workforce Framework



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2258, G4A: How would you describe your agency's adoption of the NICE Cybersecurity Workforce Framework as the standard set of required tasks and knowledge, skills, and abilities (KSAs) regarding the cybersecurity workforce?

24% of respondents claim their organization's cloud migration was enabled by FedRAMP's security controls

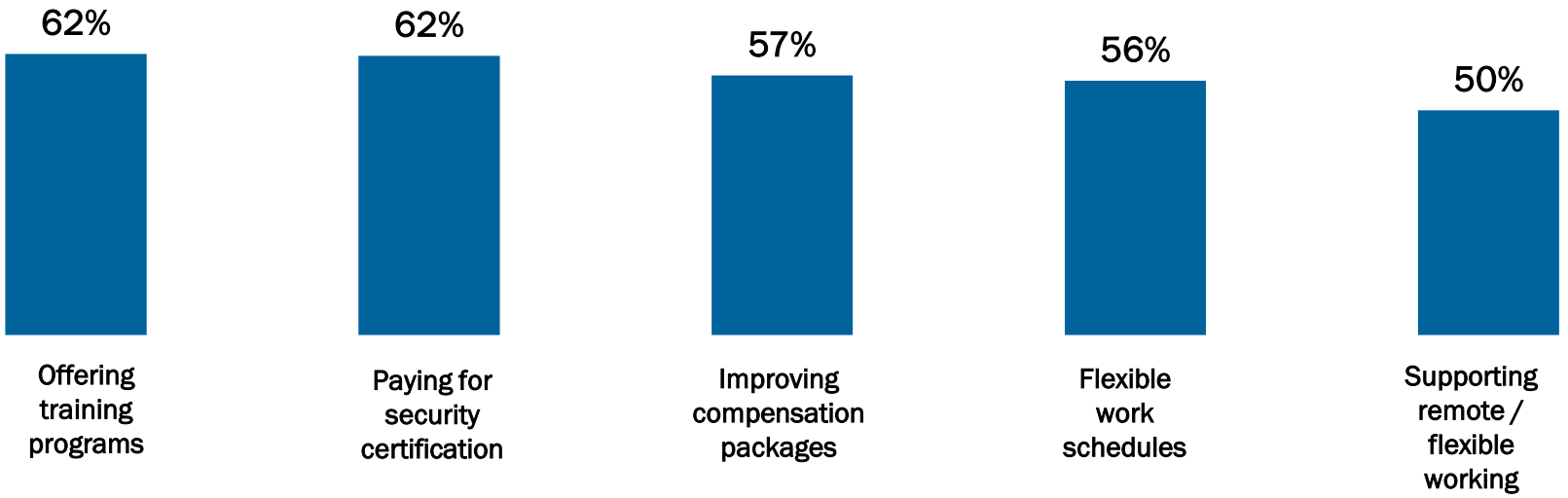


Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2258
G5: Have FedRAMP's baseline security controls enabled your agency to migrate systems more securely to the cloud?

Workforce & Funding

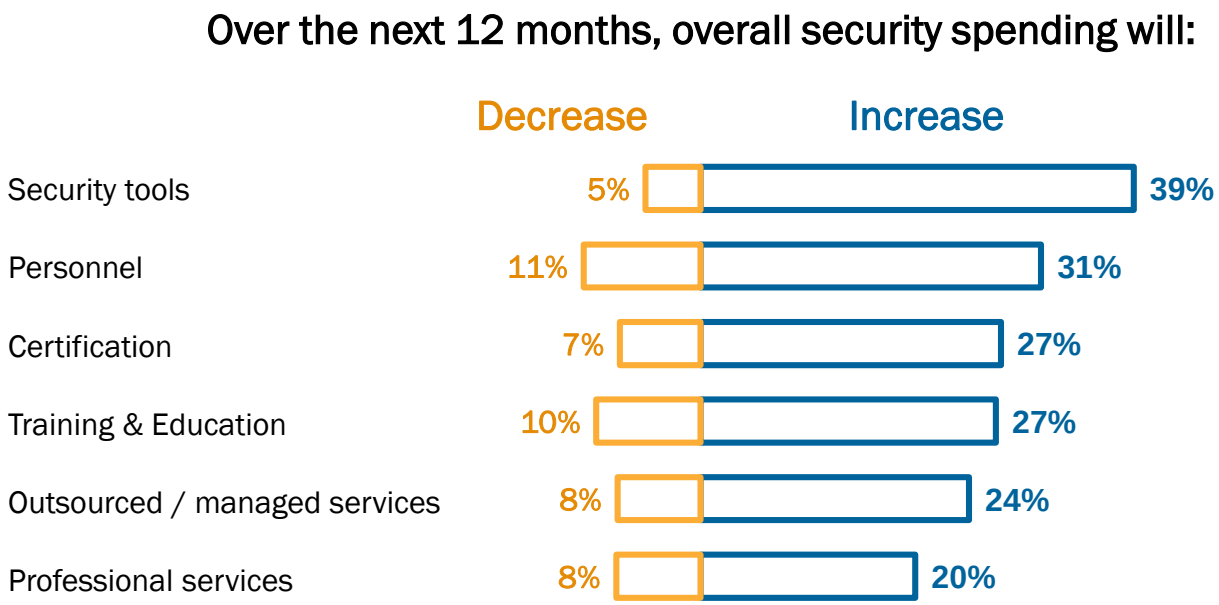
Keys to retention: training/certification, better compensation, flexibility

Top 5 initiatives seen as important for retention of information security professionals
(% of very important)



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620
Q27: How important are each of the following initiatives for the retention of information security professionals at your organization?

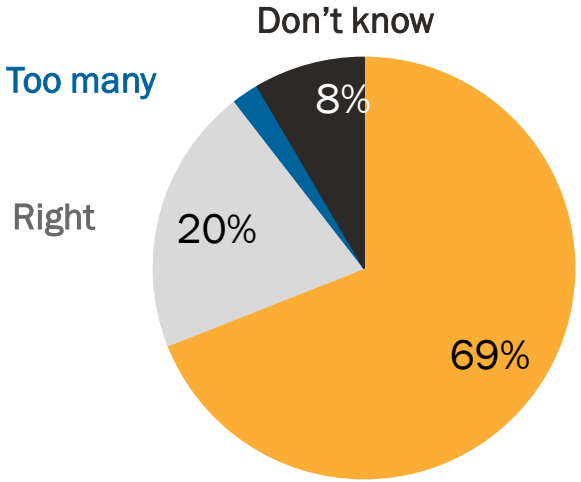
Spending Outlook



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620
Q17: Do you expect overall information security spending at your organization to increase, decrease, or remain the same over the next 12 months?

Top reasons for workforce shortage

Assessment of number of information security workers in organization



Too few

Why?

① Difficult to find qualified personnel

② Difficult to retain security workers

③ Insufficient understanding of req. for inf. security

Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620, Q28A: Would you say that your organization currently has the right number of information security workers, too few, or too many?; N (2017)=1808, Q28D: What are the reasons that your organization has too few information security workers?

Over half expect an increase in # of workers

Expected change in number of information security professionals in organization within 1Y

Increase 64%

Same 32%

Decrease 4%

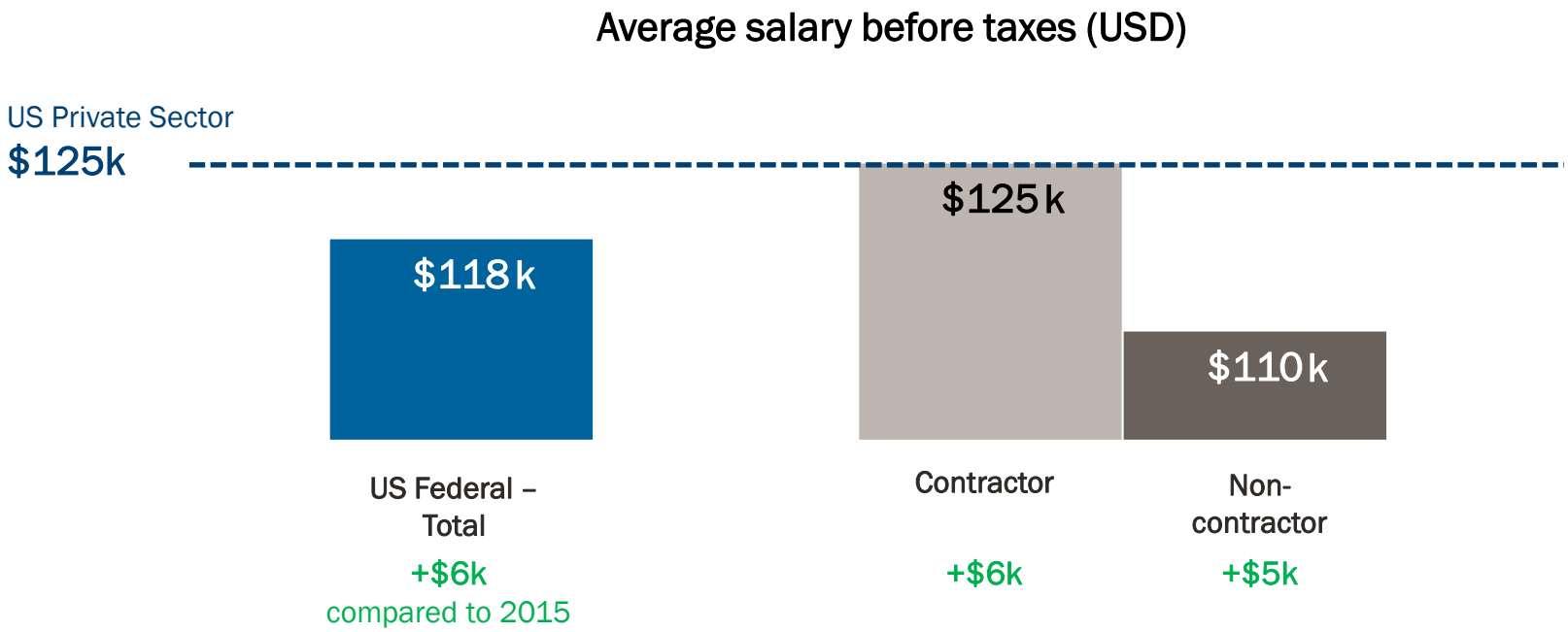
Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=418
Q19C: Over the next 12 months, do you expect the number of information security professionals in your organization to: increase, decrease, or remain the same?

Impact of shortage

Shortage of information security workers greatly impacts:
(% of great and very great impact)

Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=1808
Q28E: What is the impact of your organization's shortage of information security workers on each of the following? – Top two box scores

Fed salary increases, remains below private sector

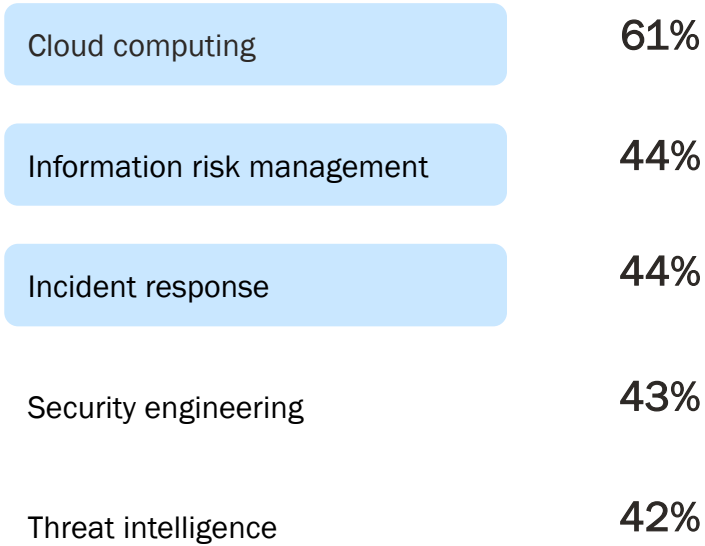


Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (US Fed, 2015/2017)=1826/2620, N (US Fed Contractor, 2015/2017)=894/1422, N (US Fed, Non-contractor, 2015/2017)=932/1198 Q61: Which of the following includes your current annual salary in U.S. dollars before taxes?

Skills, Training & Education

Cloud remains highest in demand for training/education

Top 5 areas of information security with growing demand for training & education within next 3Y



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620
Q23: In which areas of information security do you see growing demand for training and education within the next three years?

Keys to attracting new hires

Top 5 most effective recruitment incentives in attracting new cybersecurity hires

Certification / Training / Education Reimbursement	32%
Flexible Work Schedule	31%
Pay Incentives: Recruitment, Relocation, Retention, etc.	30%
Direct Hire Authority	28%
Hire Consultants / Contractors	19%

Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2258 G1: Which cybersecurity workforce recruitment tools has your agency found to be effective in attracting new hires?

Varying perspectives on which skills are needed

Employees think these are the key skills needed for advancing career:
(Top 3 skills to acquire)

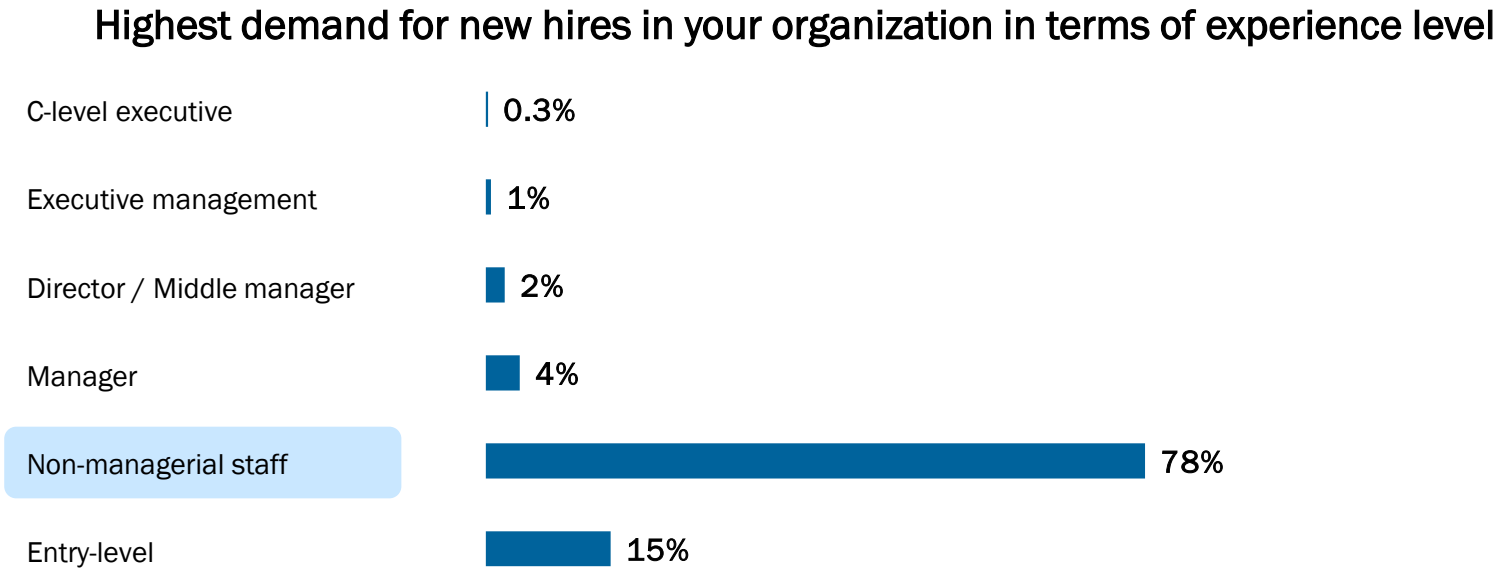
Cloud computing	60%
Risk assessment and management	42%
Governance, risk management, compliance (GRC)	38%

Hiring decision makers seek:
(Top 3 skills looked for)

Communications skills	69%
Analytical skills	60%
Risk assessment and management	50%

Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620, Q24A: What are the skills and competencies you will need to acquire or strengthen over the next 3 years to advance your career?; N (2017)=496, Q25: When you hire new employees, what are the skills and competencies you look for in a candidate?

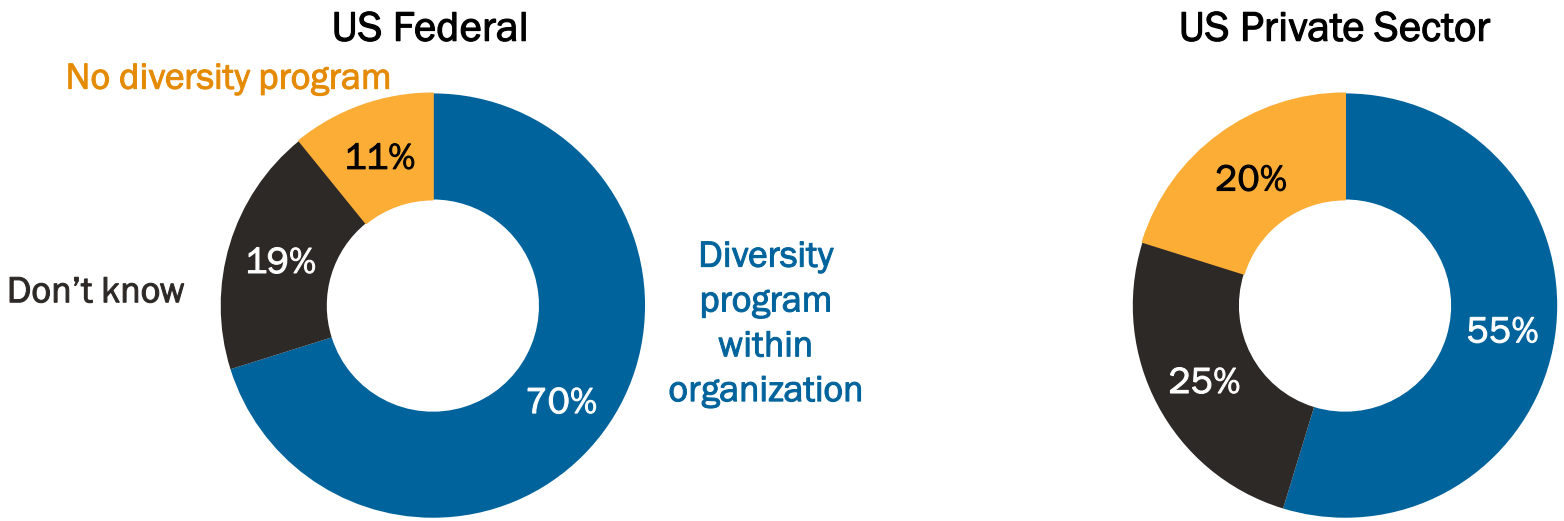
78% of respondents claim highest demand for new hires exist in non-managerial staff segment



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2579
Q22: Thinking of your organization, at what experience level is there the most demand for new hires?

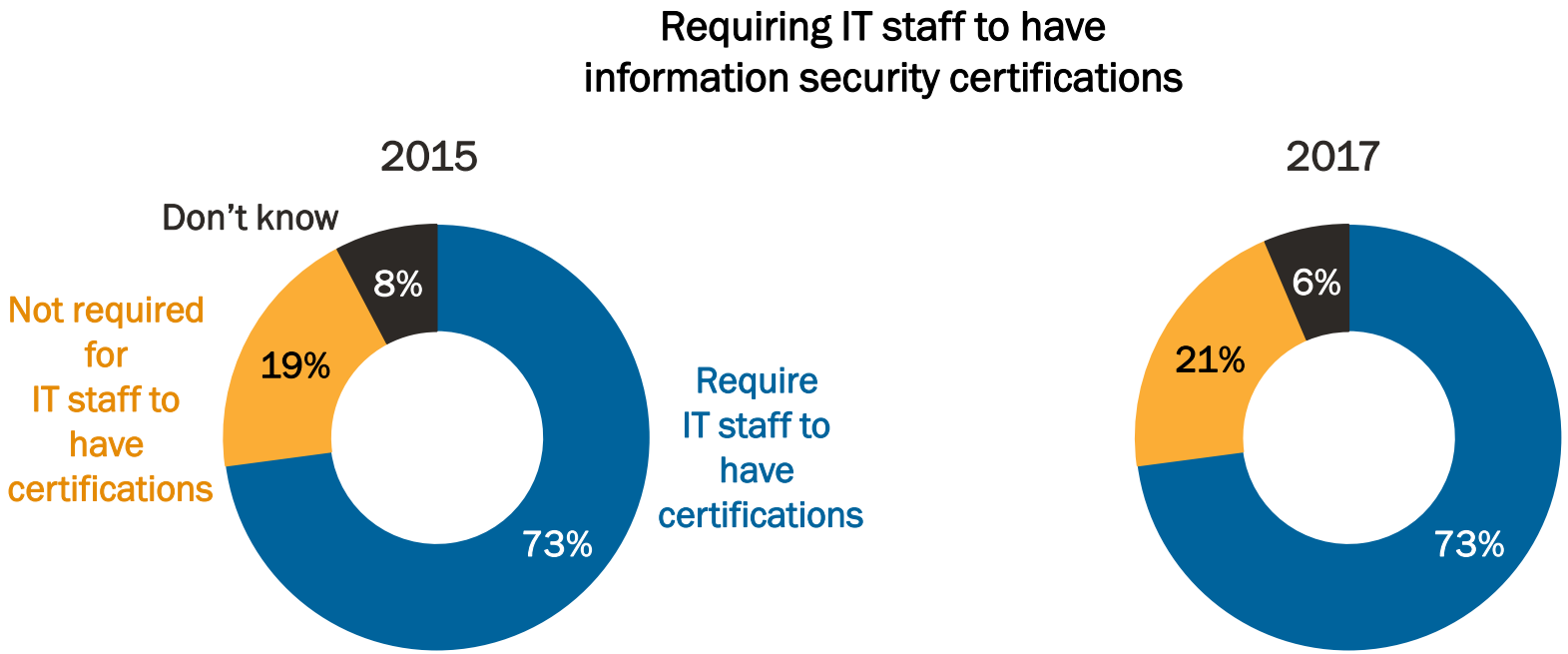
Government offers greater diversity opportunity

Having a diversity program that encourages hiring from underrepresented groups in information security



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620, Q39: Does your organization have a diversity program that specifically encourages the hiring of individuals from underrepresented groups in information security? Underrepresented groups could be defined by categories such as ethnicity, gender, religious minority or military veteran.

Requirement of certification remains unchanged



Source: Frost & Sullivan, The 2017 Global Information Security Workforce, N (2017)=2620, Q20A: Does your organization require its IT staff to have information security certifications?

Summary of Conclusions

Conclusions #1

- Organizations need to ramp up their benefits strategy if they're going to successfully compete for cybersecurity talent. Respondents say that the top initiatives recruiters and HR teams need to undertake to both attract new information security professionals and retain existing ones are:
  - Offering training programs
  - Paying for security certification
  - Improving compensation packages
  - Providing flexible work schedules
  - Supporting remote/flexible working

Conclusions #2

- There is ongoing need for front-line experience within the cybersecurity workforce, as 78% of respondents say that the greatest demand for new hires within their organizations is at the non-managerial staff level.

  The low demand (15%) for entry-level personnel suggests that, given the government's strained funding and need for more training budget, those with experience who can hit the ground running are the preferred hire.

Conclusions #3

- In competing with the private sector for skilled professionals, hiring women and those from underrepresented groups should be a key component of the government's talent acquisition strategy given that 70 percent say their organization offers a program that encourages diverse hiring in information security, compared to just 55 percent in the private sector.

Conclusions #4

- Federal agencies, in particular, are rising to the challenge in an increasingly threatening environment, with 50% of respondents stating that their agency's security has actually gotten better in the last year, while just 4% say that it's gotten worse.

The reasons for the improvement?
Better security awareness, improved understanding of risk management and more effective security standards.

Conclusions #5

- Security needs to be on everybody's to-do list, as the vast majority of information security professionals (81%) now say that making non-technical staff aware of security issues is very important or somewhat important to effectively securing an organization's infrastructure, a jump of 21% in just two years.

Special thanks to the Center for Cyber Safety and Education and (ISC)^2 for sponsoring this *U.S. Government Perspective* report and to Booz Allen Hamilton for being the report's supporting organization.

For more information, please visit:
www.IAmCyberSafe.org/GISWS