Market Connections
Research you can act on.

Unisys
Digital Trust Survey
Summary Report

Report Publication January 31, 2018

Background & Demographics

Research Objectives and Methodology

The objectives of the Unisys Digital Trust Survey are to:

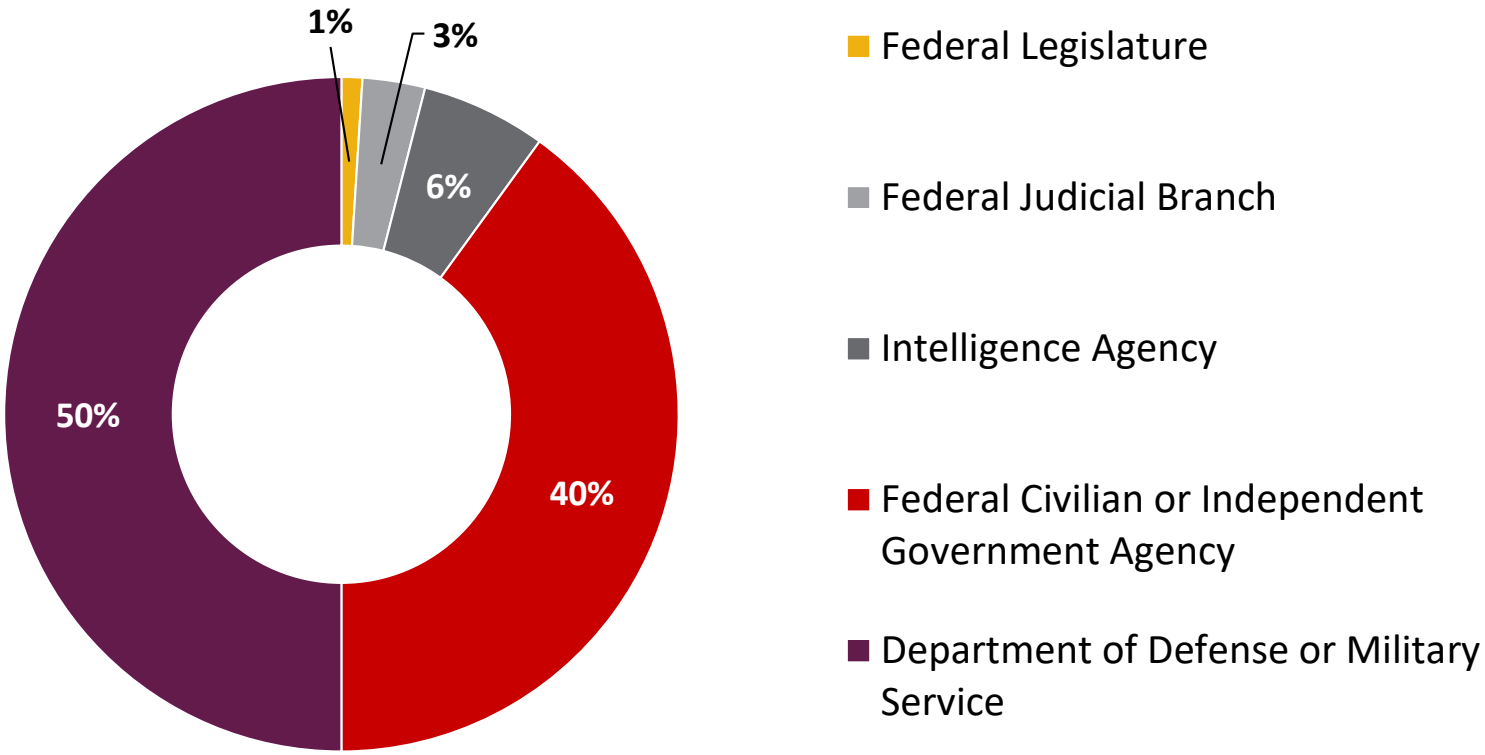
- Gauge IT security confidence and vulnerability
- Identify IT security challenges, concerns, and threats facing federal agencies
- Determine identity management importance, benefits, and challenges

From July 18 to August 08, 2017, 200 federal government decision makers (101 federal civilian and 99 DoD/military) participated in an online survey that averaged eight minutes in length.

Throughout the report, significant differences are noted with a symbol or gold box. Due to rounding, graphs may not add to 100%.

Current Employer

- Half of respondents work at federal civilian or independent agencies (including federal judicial, legislative and intelligence agencies). The other half work for DoD or military branches.

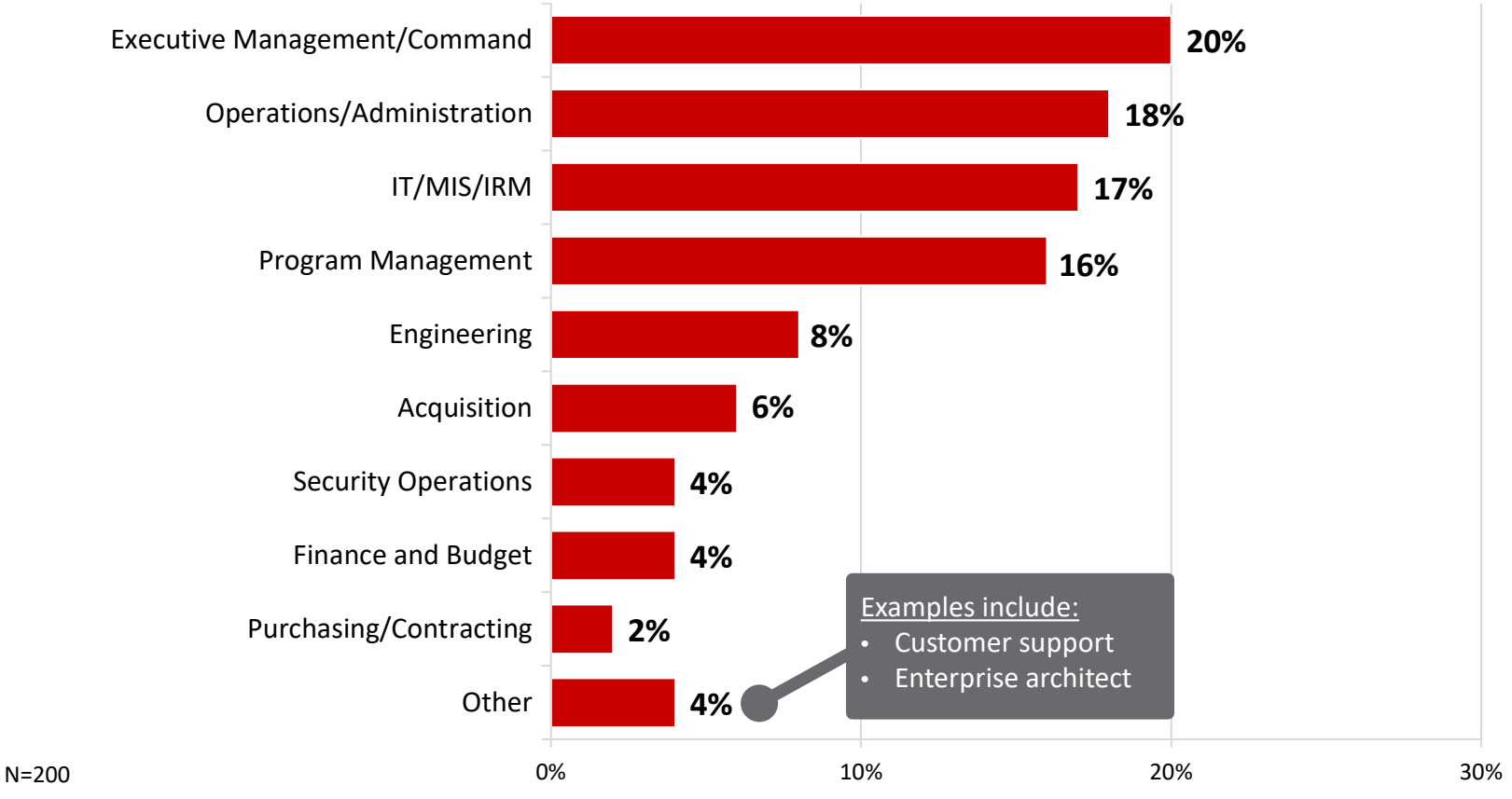


N=200

Q *Which of the following best describes your current employer?*

Organization Role

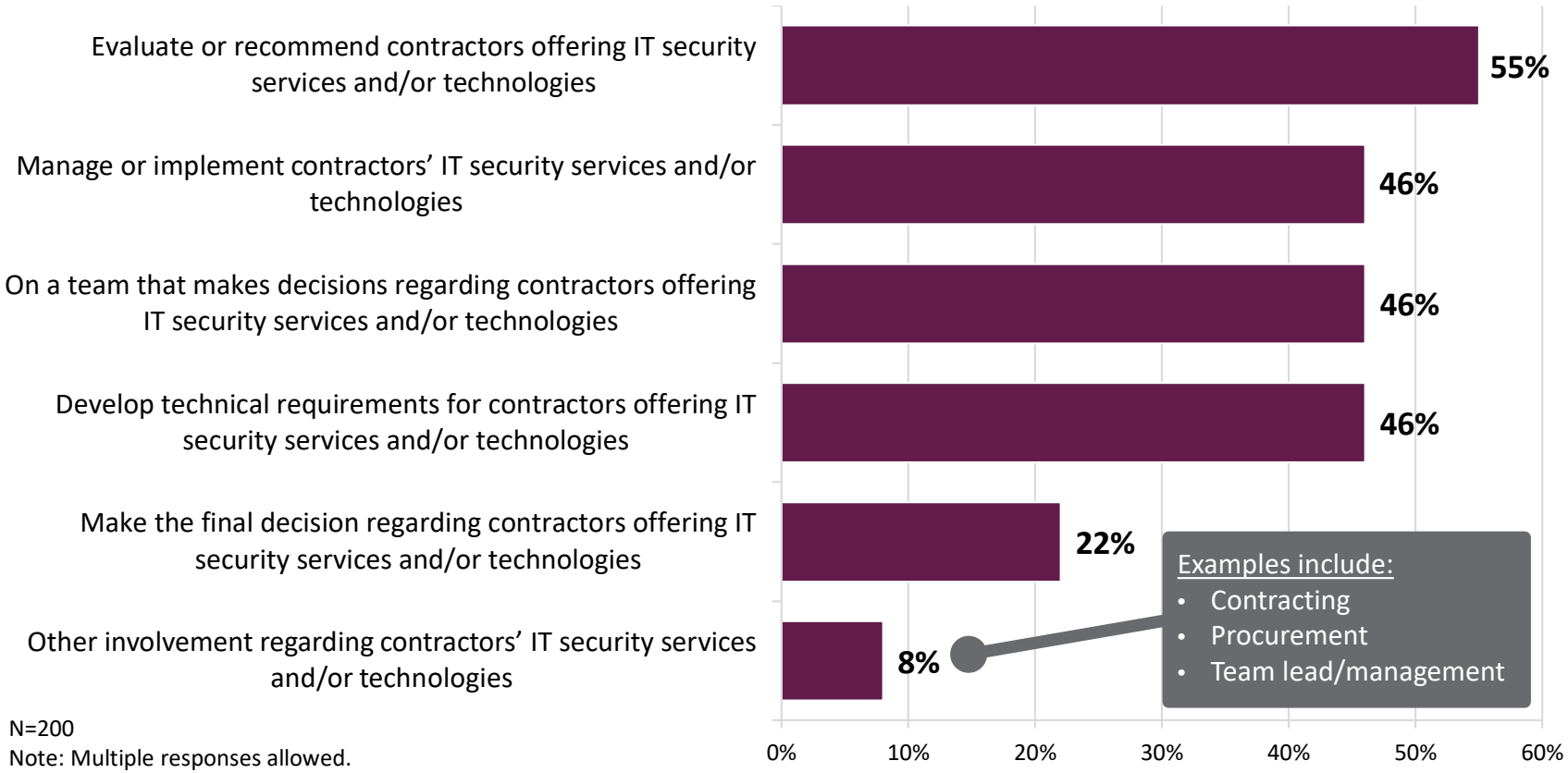
- A diverse selection of job roles is represented in the sample, with the highest proportions in executive management/command, operations/administration, IT/MIS/IRM, and program management.



Q *Which of the following best describes your role in your organization?*

Decision-Making Involvement

- More than half of respondents evaluate or recommend contractors offering IT security services and/or technologies. Nearly a quarter make the final decision regarding contractors in this area.



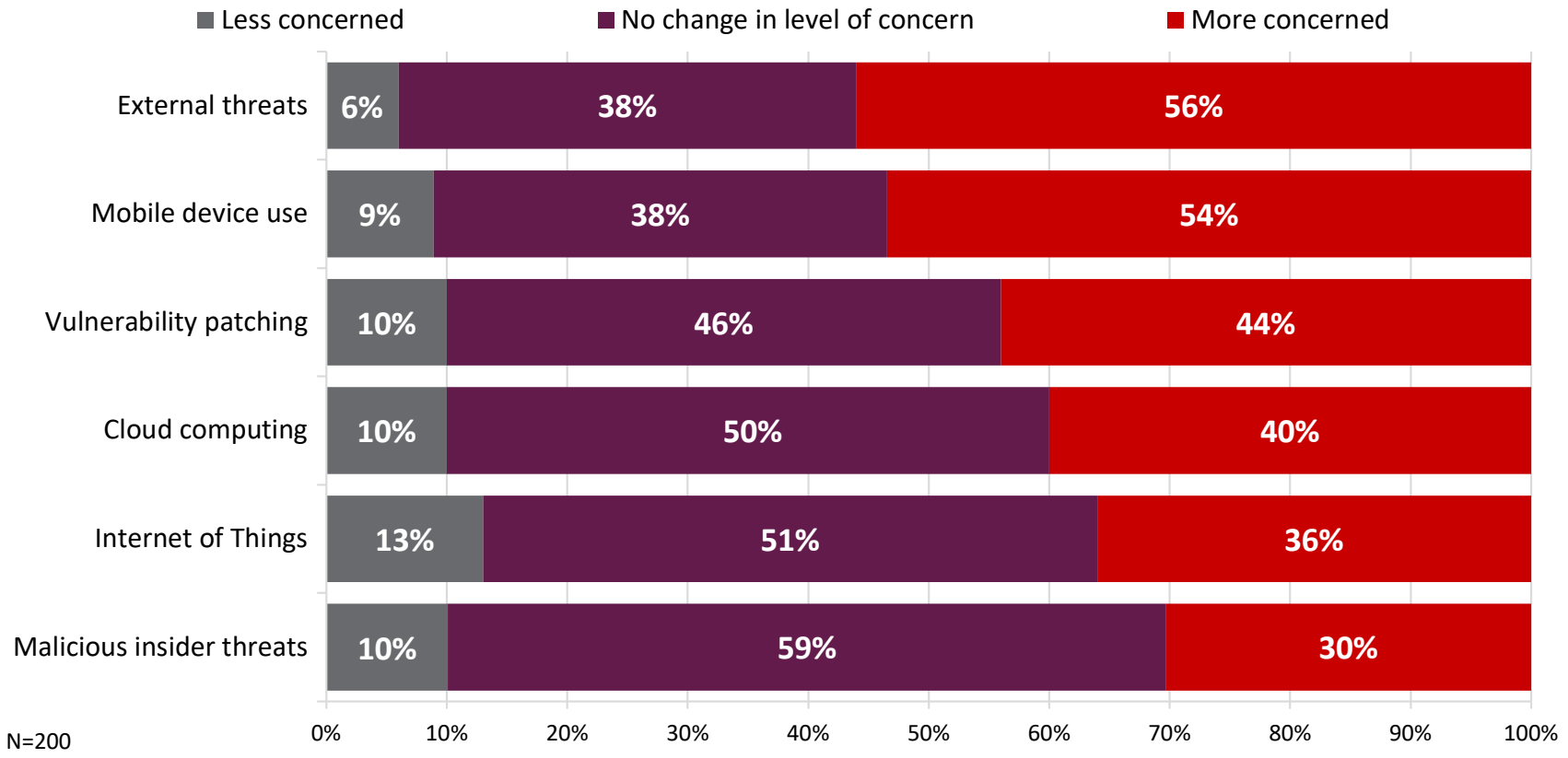
N=200
Note: Multiple responses allowed.

Q *How are you involved in your agency's selection and/or management of government contractors that provide IT security services and/or technologies? (select all that apply)*

Study Results

IT Security Concerns Over the Last 12 Months

- The most commonly mentioned areas of greater IT security concern in the last 12 months are led by external threats, mobile device use and vulnerability patching.

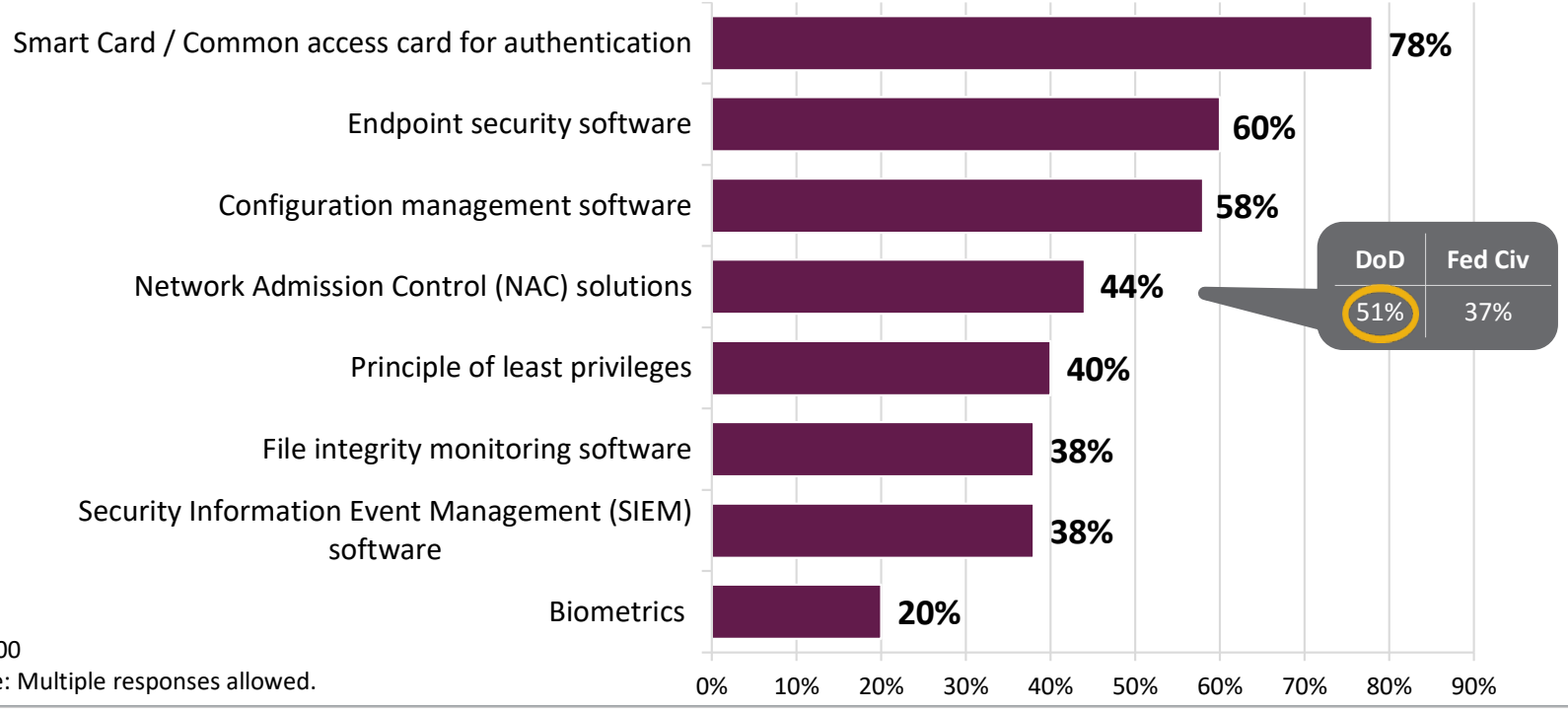


N=200

Q *In the last 12 months, how, if at all, has your organization's concern changed for the following as it relates to your IT security environment?*

Security Products and Practices in Use

- More than half of respondents indicate the most widely used security products or practices currently in use at their agencies are smart cards, endpoint security software, and configuration management software.
- DoD respondents are significantly more likely than their civilian peers to use NAC solutions.



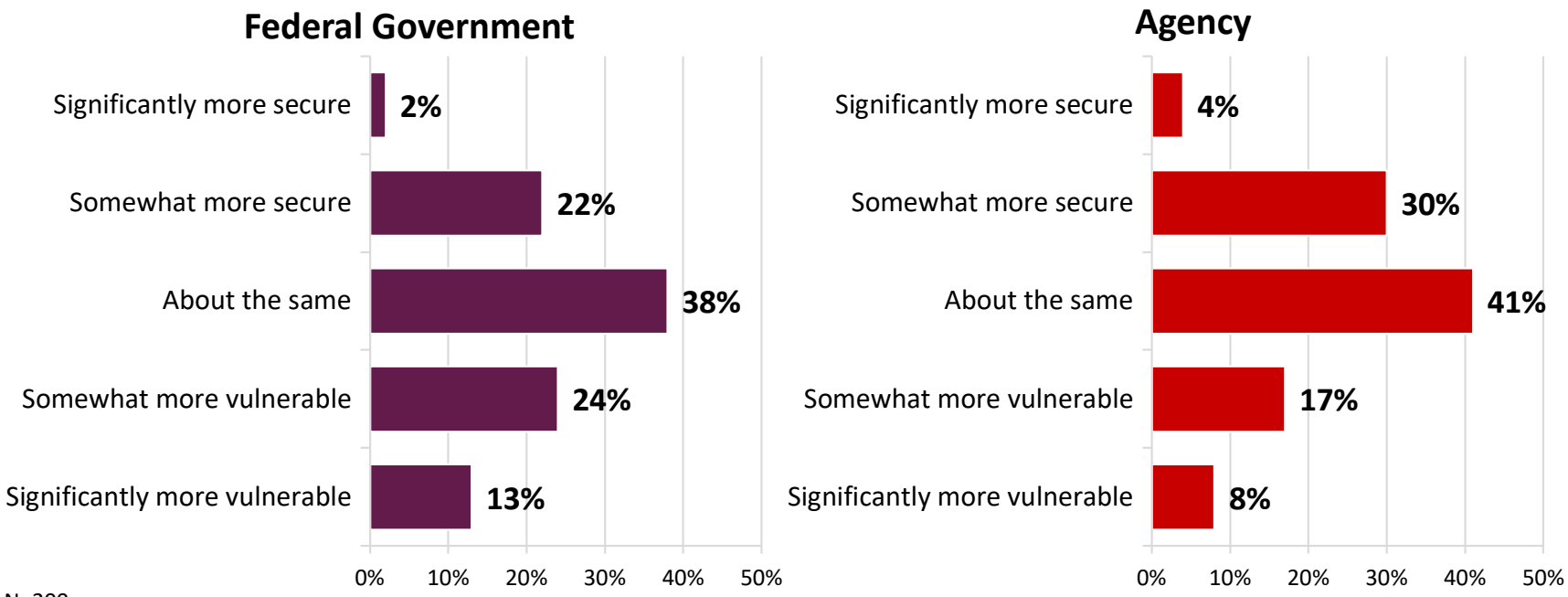
N=200
Note: Multiple responses allowed.

Q *Which of the following security products or practices are currently in use in your organization? (select all that apply)*

= statistically significant difference

IT Security Posture Compared to 12 Months Ago

- Compared to 12 months ago, one-quarter of respondents think the federal government's broader IT security posture is somewhat or significantly more secure, versus nearly four in ten thinking it is more vulnerable. They appear more positive about their own agency's posture, where one-third believe their agency is somewhat or significantly more secure – although a quarter think it is more vulnerable.



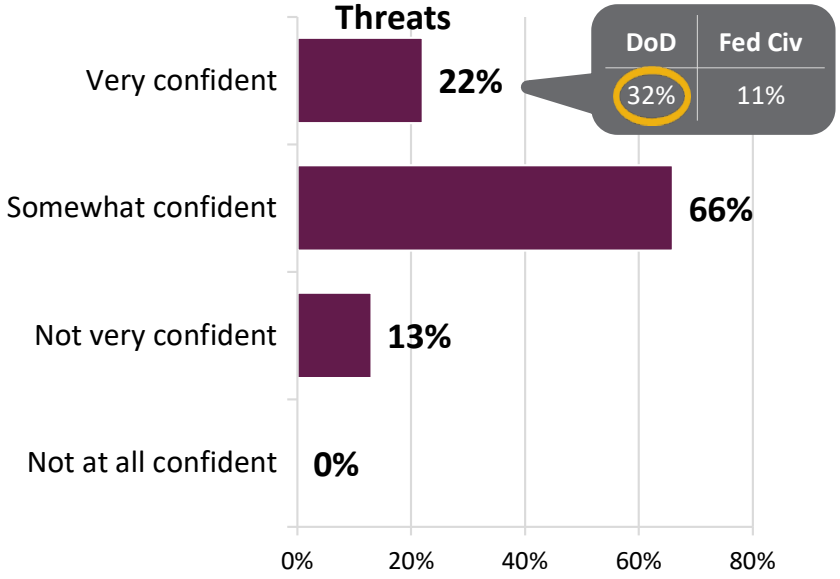
N=200

Q *In your opinion, how would you describe the federal government's broader IT security posture compared to 12 months ago?*
In your opinion, how would you describe your agency's IT security posture compared to 12 months ago?

Current Confidence in Agency's Ability

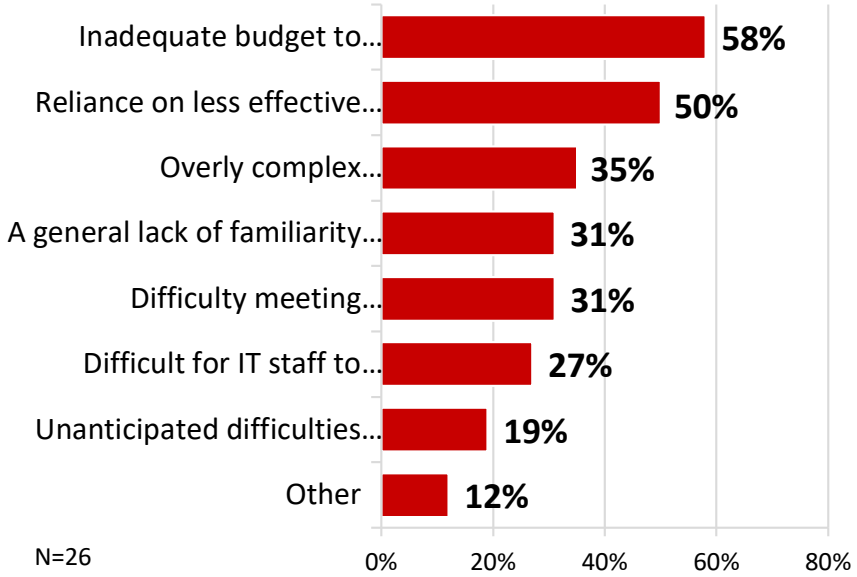
- Less than a quarter are very confident in their agency's ability to prevent IT security threats. However, DoD respondents are three times as likely as their civilian colleagues to express such high confidence.
- More than half cite inadequate budgets and reliance on legacy systems for their lack of confidence.

Confidence in Agency's Ability to Prevent IT Threats



N=200

Reasons for Lack of Confidence



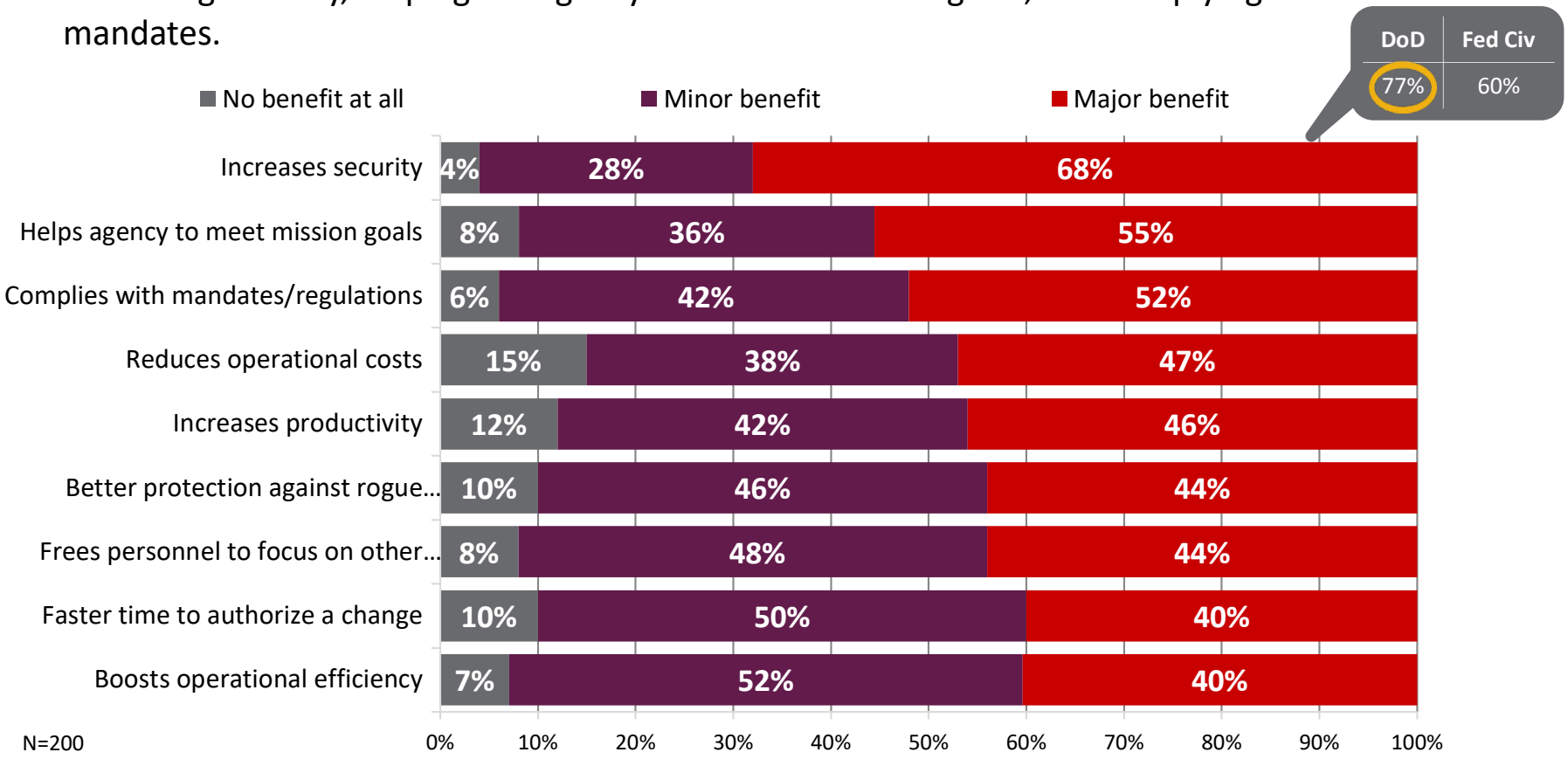
N=26
Note: Multiple responses allowed.

Q *How confident are you in your agency's current ability to prevent against IT security threats?*
What are the reasons behind your lack of confidence in your agency's ability to protect itself? (select all that apply)

= statistically significant difference

Identity Access Management System Benefits

- The most commonly cited major benefits of an identity access management system are increasing security, helping the agency to meet its mission goals, and complying with mandates.

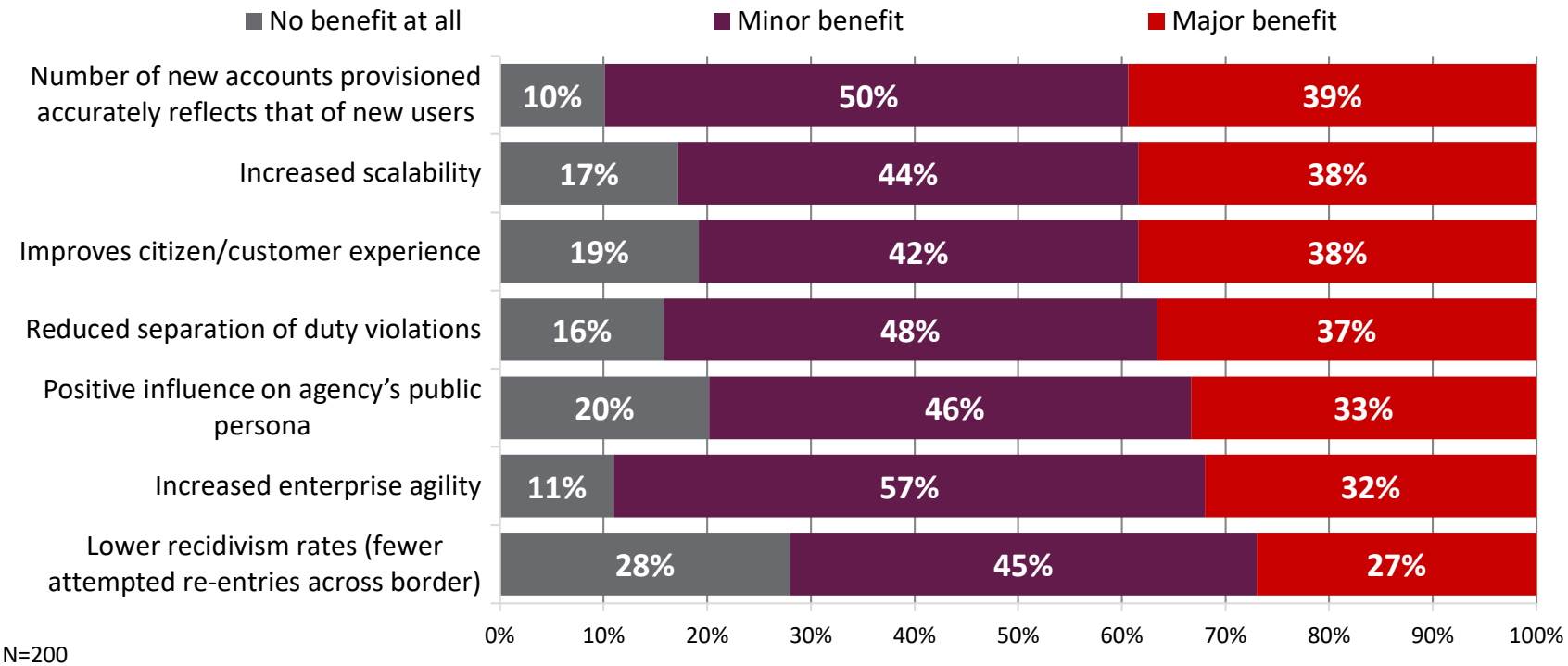


Q *How much, if any, do you see the following as a benefit to implementing an identity access management system at your agency for both your employees and contractors and citizens using your agency's services?*

= statistically significant difference

Identity Access Management System Benefits (Continued)

- An identity access management system is seen by more than four in ten to have no benefit at all on lowering recidivism rates.

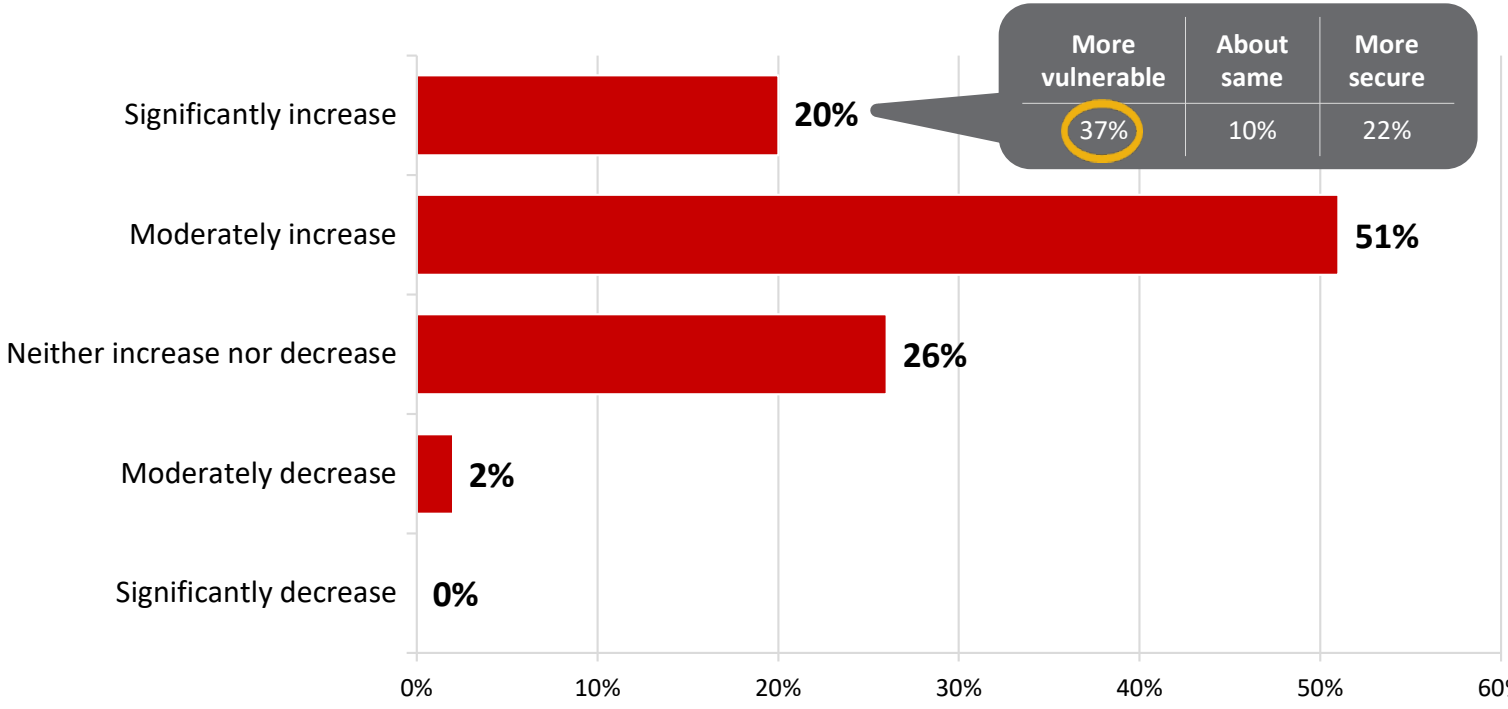


N=200

How much, if any, do you see the following as a benefit to implementing an identity access management system at your agency for both your employees and contractors and citizens using your agency's services?

Anticipated Change in IT Security Threats Over the Next 12 Months

- Over the next 12 months, one in five respondents, rising to nearly four in ten among those that feel their agency's security posture is more vulnerable compared to 12 months ago, believe IT security threats against their agency will significantly increase.

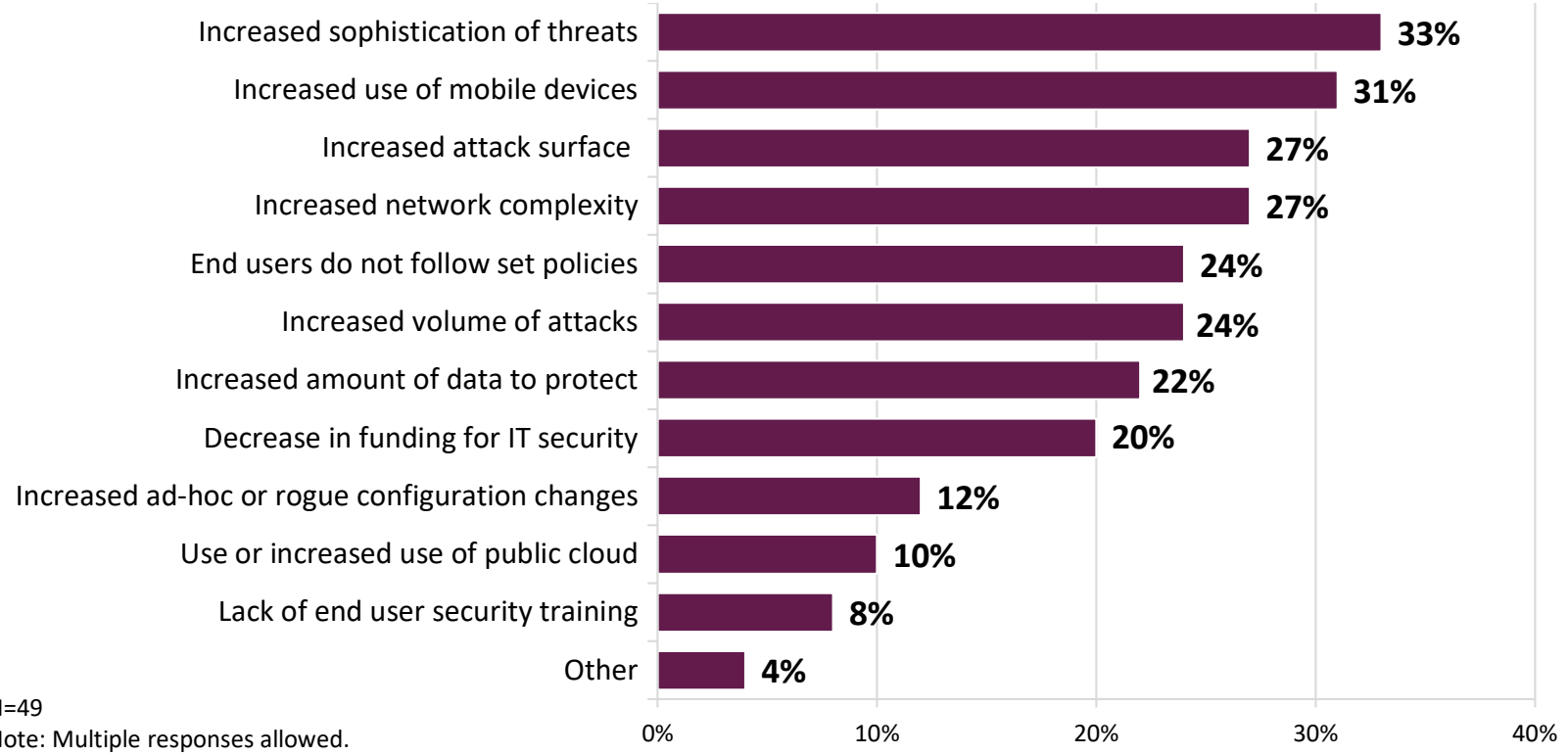


N=200

Q *Over the next 12 months, do you anticipate IT security threats against your agency to increase, decrease, or stay the same as now?* = statistically significant difference

Reasons for Agency's Increased Vulnerability

- The most common reasons behind respondents' feelings that their agency is more vulnerable include the increased sophistication of threats, and the increased use of mobile devices. A broad mix of other reasons reveals the wide scope of this vulnerability.

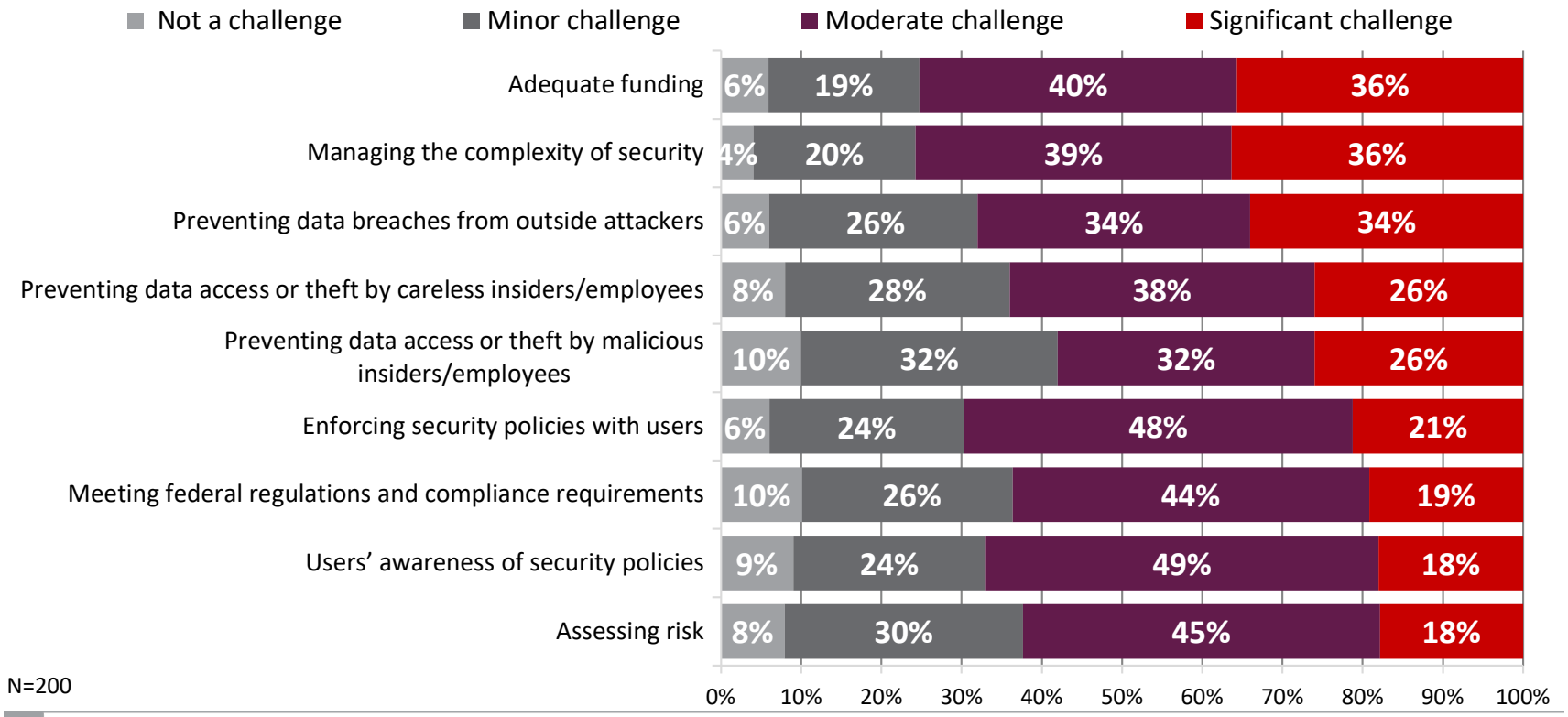


N=49
Note: Multiple responses allowed.

Q *What do you consider the main reasons for your agency's increased vulnerability? (select top three)*

IT Security Challenges

- More than one-third of respondents point to adequate funding, managing the complexity of security, and preventing data breaches by outside attackers as significant challenges to the IT security of their agency.

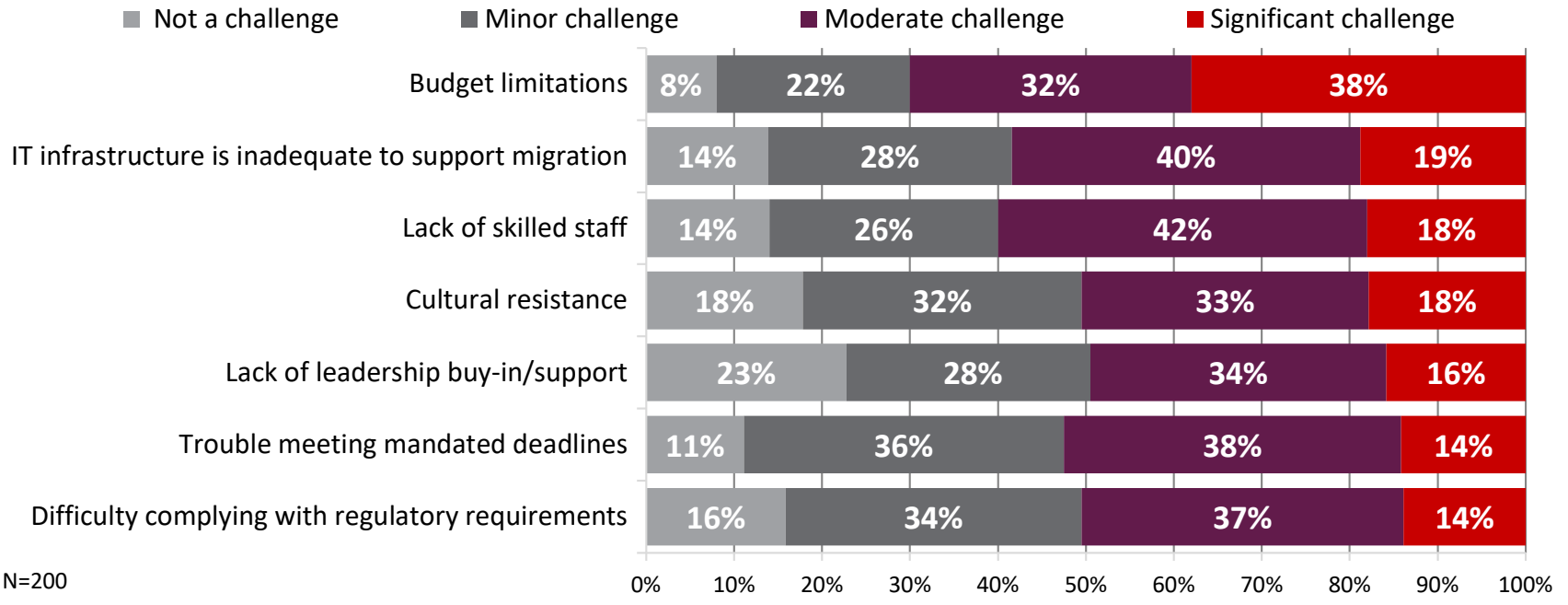


N=200

Q *To what extent are the following a challenge to the IT security of your agency?*

Challenges Migrating to an Identity-Based Security Management System

- The most commonly cited significant challenge agencies face to migrate to an identity-based security management system are budget limitations – twice the proportion of a second tier pointing to IT infrastructure inadequate to support migration, lack of skilled staff, and cultural resistance.



Q *To what degree are the following items a challenge to your agency's effort to migrate to an identity-based security management system?*

Challenges Migrating to an Identity-Based Security Management System: Differences

- Respondents that feel their agency's security posture is more vulnerable versus 12 months ago are significantly more likely to mention challenges related to buy-in, cultural resistance, and lack of skilled staff.

Significant Challenges to Migrate to an Identity-Based Security Management System				
Factor	Total %: Significant Challenge	Respondents' agencies' security posture versus 12 months ago		
		More vulnerable	About the same	More secure
IT infrastructure inadequate to support migration	19%	31%	17%	13%
Lack of skilled staff	18%	33%	13%	14%
Cultural resistance	18%	35%	10%	14%
Lack of leadership buy-in/support	16%	37%	10%	9%
Trouble meeting mandated deadlines	14%	27%	9%	12%
Difficulty complying with regulatory requirements	14%	31%	10%	7%

N=200

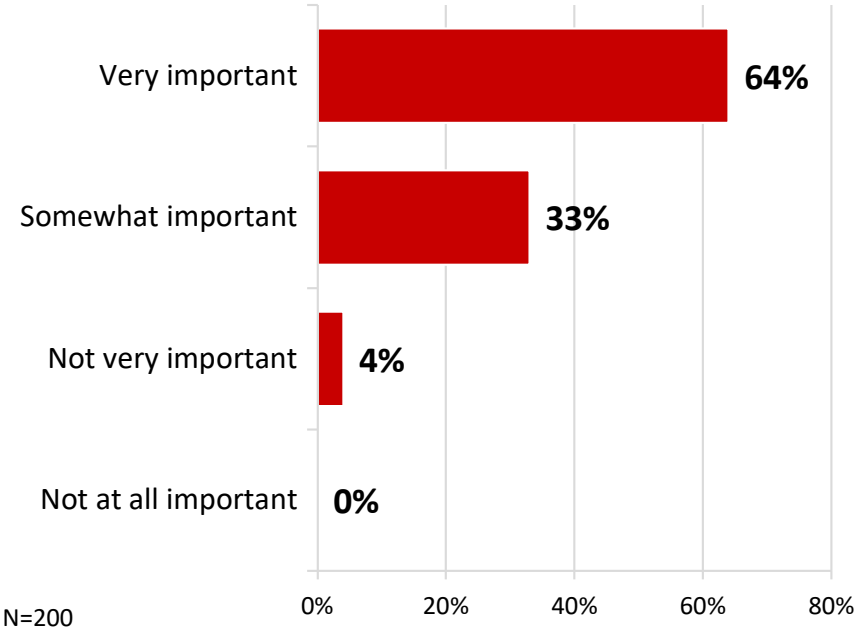
= statistically significant difference

Q *To what degree are the following items a challenge to your agency's effort to migrate to an identity-based security management system?*

Identity Management Importance and Tools

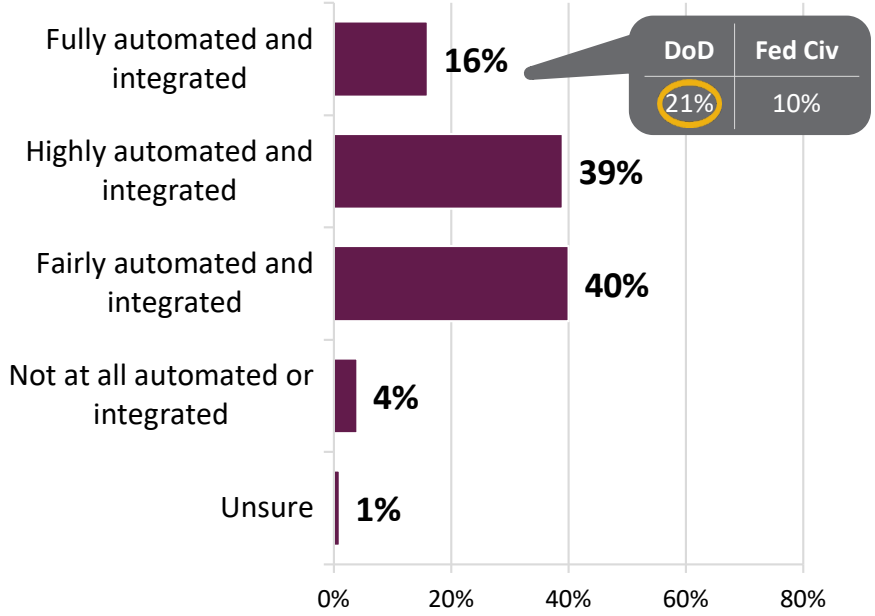
- Nearly two-thirds feel identity management systems are very important to the secure operation of their agency.
- Although nearly all respondents indicate their agency's tools are automated to some degree, very few are fully automated and integrated. DoD outpaces civilian agencies on this measure.

Identity Management System Importance



N=200

Agency's Identity Based Security Tools and Practice Environment



All things considered, how important is an identity management system to the secure operation of your agency?
How would you describe your agency's identity based security tools and practice environment?

= statistically significant difference

For more information on Unisys Digital Trust:

- Research report
- White paper
- Point of view

www.unisys.com/digitaltrust

Market Connections
Research you can act on.

DAVE GLANTZ
RESEARCH DIRECTOR

11350 RANDOM HILLS ROAD, SUITE 800 | FAIRFAX, VA 22030

571.257.3643

DaveG@marketconnectionsinc.com