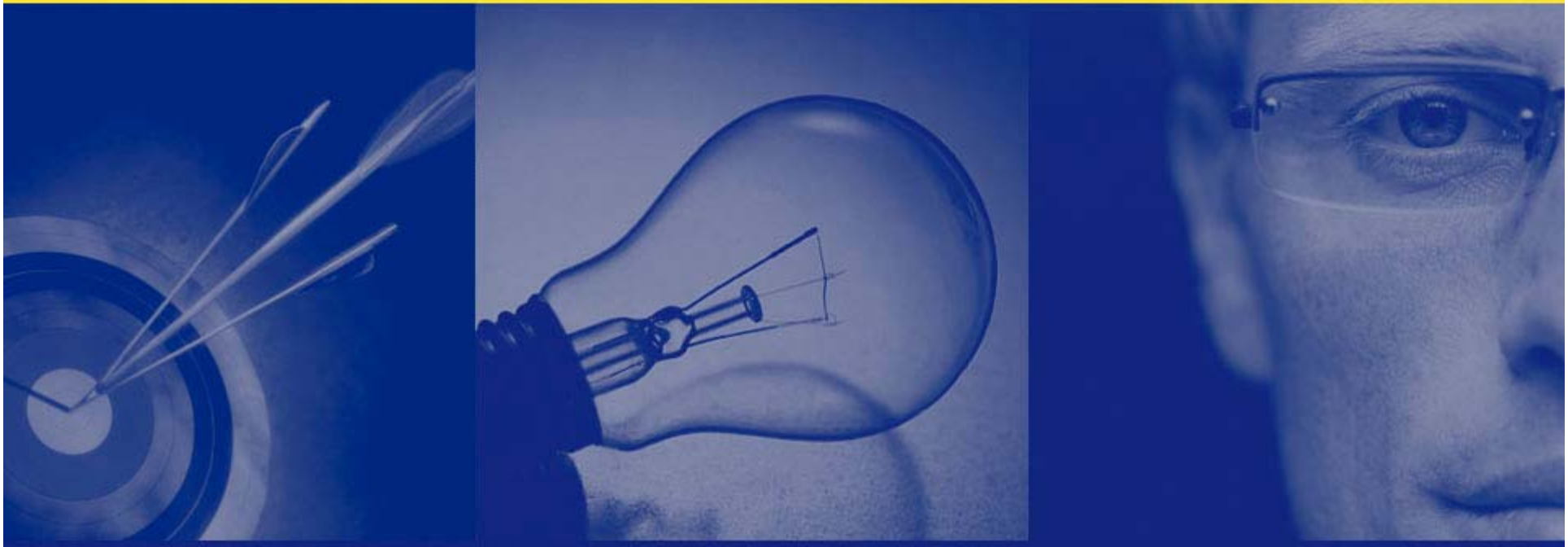
The Urgency to Maintain Security Has Never Been Greater



Quest Software

2008 Identity Management Government Survey

Agenda

- Objective & Methodology
- Executive Summary
- Noteworthy Findings
- Summary
- Quest Software Puts Government Agencies on the Runway for Successful Identity Management

"The *Identity Management Government Survey* reveals that the runway for government agencies is getting shorter and shorter, and this critical security concern cannot await a utopian solution .

The most significant measure government agencies can take today is to leverage prevalent infrastructure investments, such as Microsoft Active Directory, to serve as a centralized identity repository and immediately begin working towards single/reduced sign-on."

-- Paul Garver, Vice President of Public Sector, Quest Software

QUEST SOFTWARE® PUBLIC SECTOR
Government & Education Solutions

Objective & Methodology

- Objective
  - To get a pulse on government IT professionals' perceptions of compliance with IdM mandates and for the first time, reveal the barriers to success, and the impact on national security, critical public infrastructure, and personal security
- Methodology
  - Online surveys were completed by 474 government IT professionals from federal civilian, defense, state, local and municipal government agencies (margin of error is +/- 4.49% at the 95% confidence interval)
  - Pursuant, a Washington, D.C.-based public opinion research firm, conducted the survey in January 2008
  - Respondents included government IT decision makers with the following job functions: C-Level Management/Command; Executive/Senior/Comptroller/Division Management; Programs/Project Management; Administration/Operation Management; and IT/IS/DP/Network/System Management
  - Respondents self-identified belonging to the following governmental divisions:
    - 315 Federal government/military IT professionals: 168 Federal civilian, 127 Federal military/DOD, and 20 Feds did not specify whether military/DOD or civilian
    - 117 State and local government
    - 42 respondents did not report the type of government entity they work for
- Identity management Defined
  - An integrated system of business processes, policies and technologies that enable government organizations to facilitate and control user access to critical online applications and resources. This is established to protect confidential business and personal information from unauthorized users.

Executive Summary

- The importance of identity management efforts will **increase overwhelmingly** because of the impact on national security, critical public infrastructure, and personal security.

- About **35%** of government IT professionals project that their organization or agency will be **compliant** with government identity management mandates within the next two years, while **37%** report that they **"don't know"** when their organization or agency will be compliant. This may reflect on the **challenges inherent in the complexity** of the requirements and the difficulty experienced by respondents in **juggling ongoing** and **unfunded** IdM efforts with existing priorities.

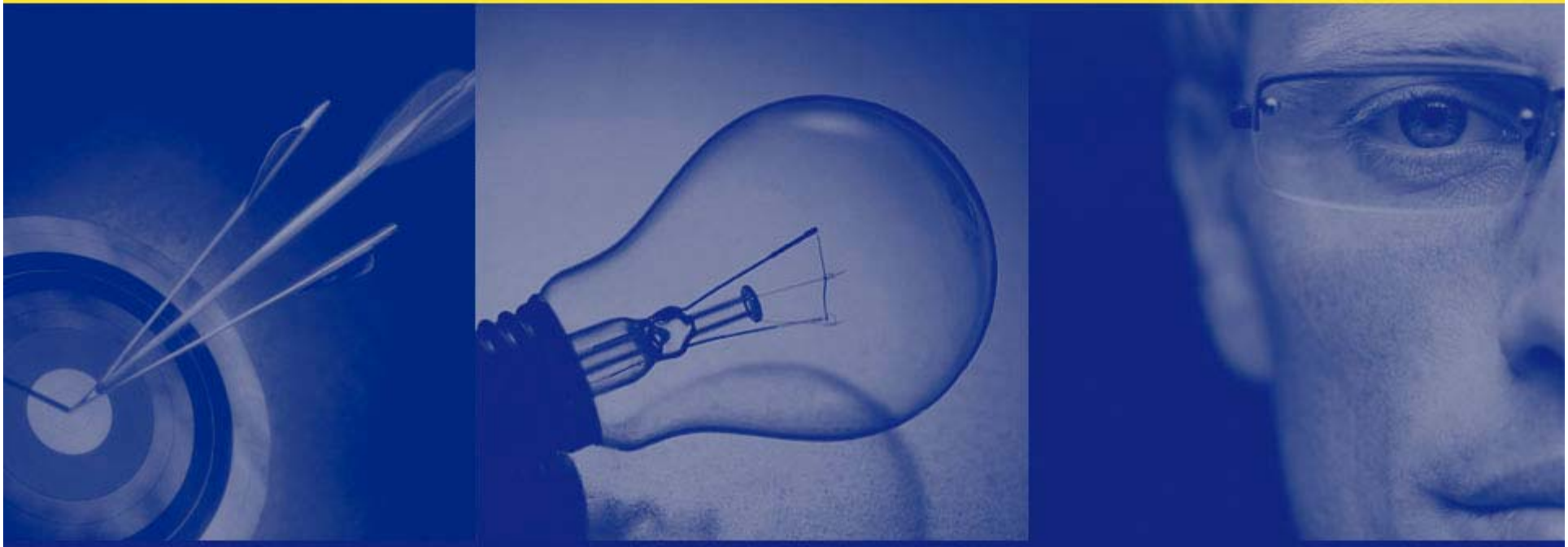
- Respondents point to real business and technology challenges that stand in the way of compliance. The top obstacles cited include the **lack of funding, technological complexity and staffing resources**.

Executive Summary

- The majority of respondents believe **Congress should play a more active role by providing more funding and/or require greater planning/collaboration** among government entities.
- Over one-half of government IT professionals believe that **national security should be the priority** even if it means that Americans' personal privacy could be negatively impacted.
- Over one-half of government IT professionals have either personally **seen or heard** about someone **violating their organization or agency's security protocols**.
- More **city, county and municipal** government IT professionals are likely to be "**very concerned**" about **compromised critical public infrastructure** than federal or state government IT professionals.
- According to about **half** of respondents, a **heterogeneous (mixed-application) environment is "very challenging" or "somewhat challenging"** for their organization or agency's IdM system.

Noteworthy Findings

QUEST SOFTWARE®
PUBLIC SECTOR



From the Quest Software 2008 Identity Management Government Survey

Increasing Data/Info Security, Followed by Compliance with Fed Mandates Top Reasons for IdM Systems

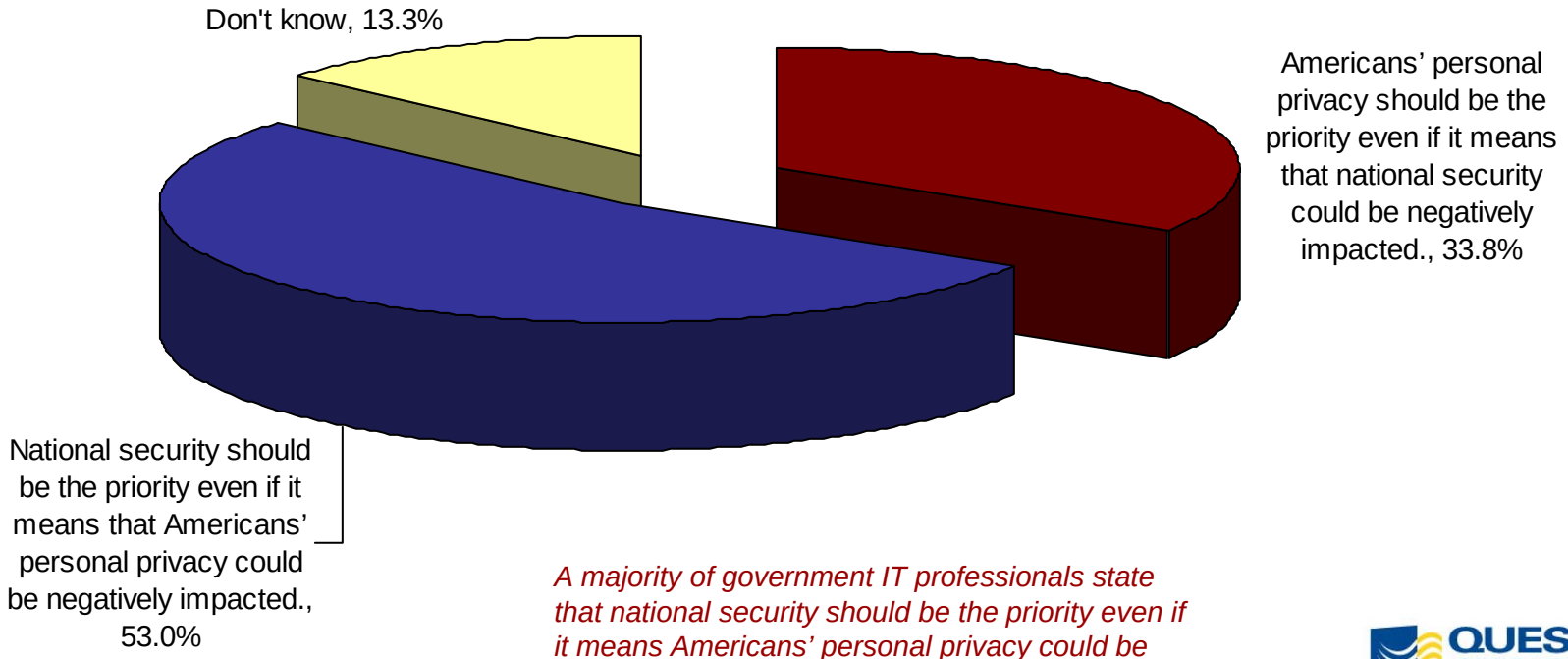
What is your organization or agency's top reason for instituting an identity management system?

Top Reason	**%**
Increase physical, data and information security	33.3%
Compliance with government mandates like HSPD-12, FIPS 201, FISMA, etc.	32.1%
Protection of personal information	19.0%
Simplify internal data systems	2.5%
None of these	3.8%
Don't know	9.3%

Increasing security (physical, data and informational) and compliance with government mandates was most frequently selected as the "top reason" for instituting an identity management system.

National Security Should Trump Personal Privacy, According to a Majority of Government IT Professionals

There is much debate about how to maintain the proper balance between personal privacy and national security. Which **comes closest** to describing your view when legislation and government mandates are being developed?

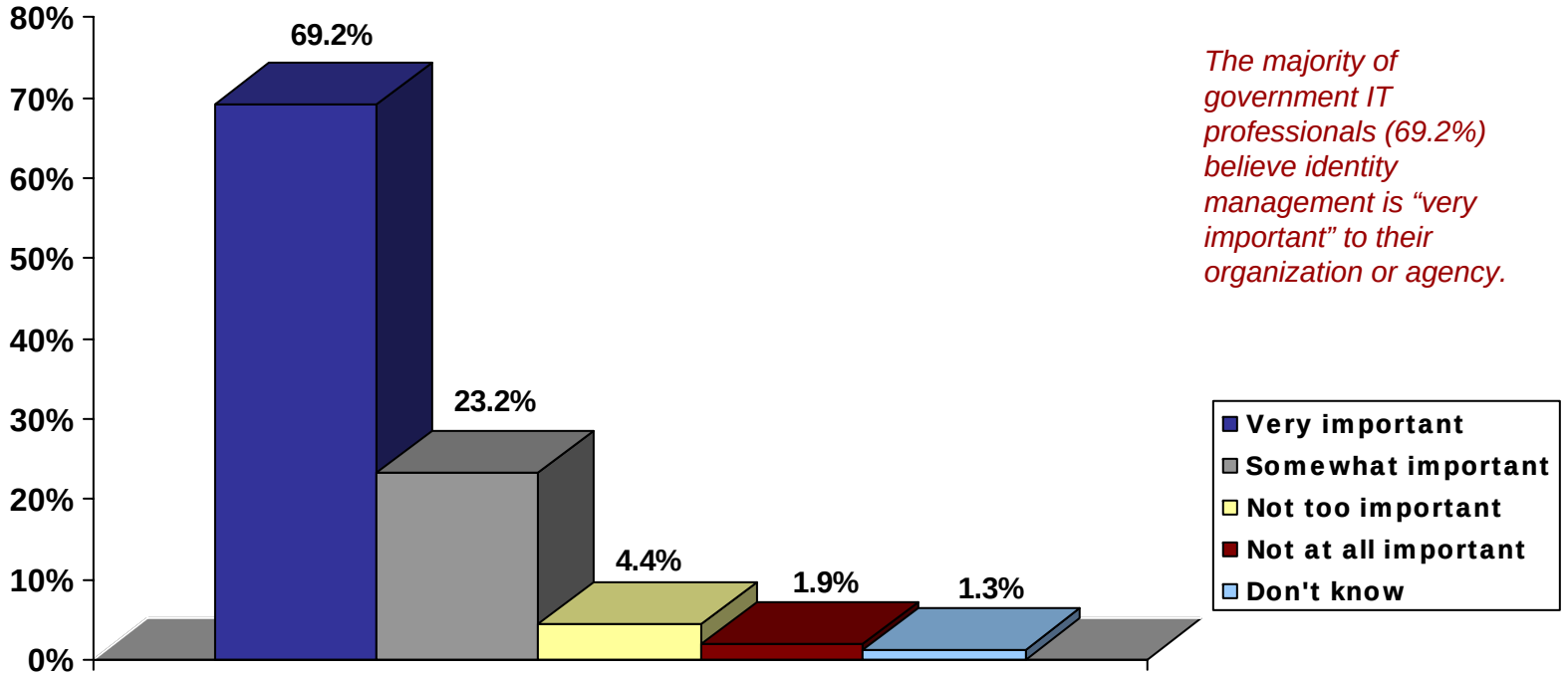


A majority of government IT professionals state that national security should be the priority even if it means Americans' personal privacy could be negatively impacted (53.0%).

QUEST SOFTWARE®
PUBLIC SECTOR
Government & Education Solutions

Identity Management "Very Important" According to the Majority of Government IT Professionals

In your opinion, how important is identity management to your organization or agency currently?

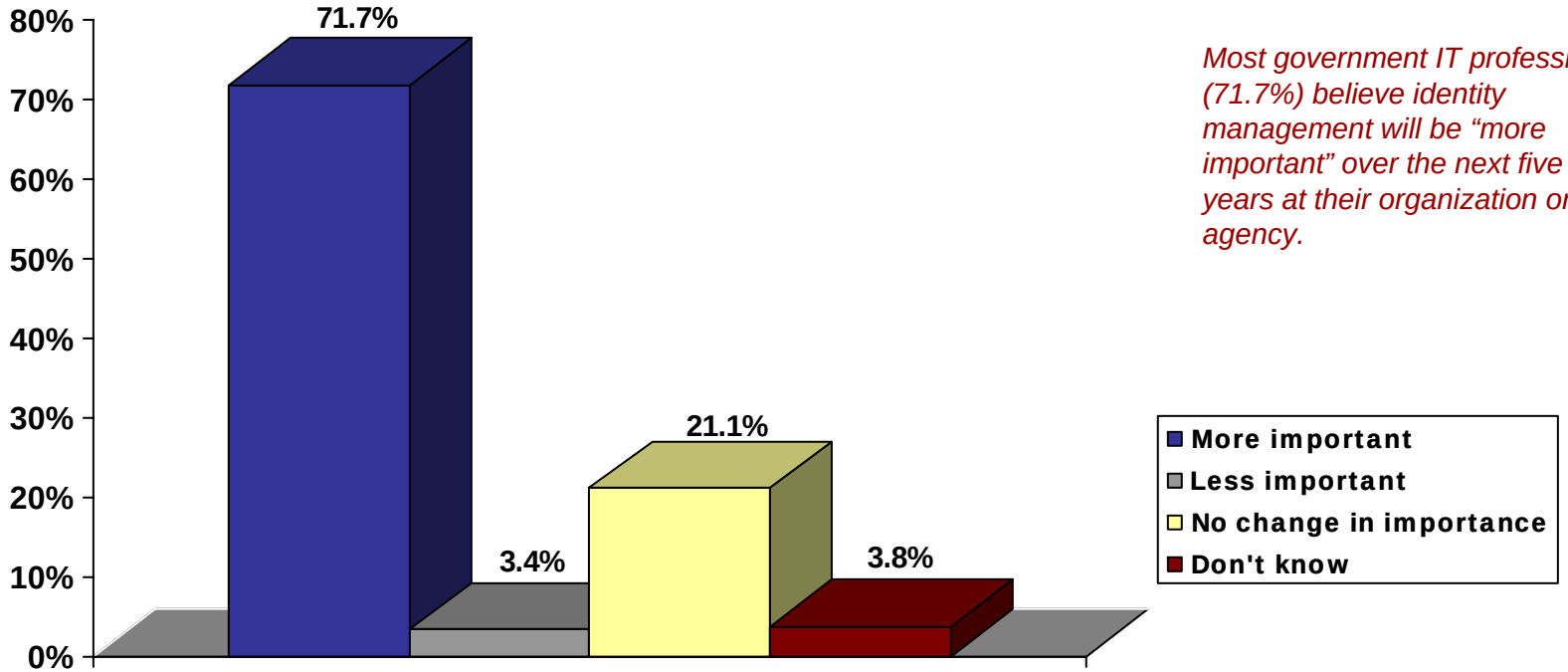


The majority of government IT professionals (69.2%) believe identity management is "very important" to their organization or agency.

QUEST SOFTWARE
PUBLIC SECTOR
Government & Education Solutions

In the Next 5 Years, Nearly 3 out of 4 Think IdM Will Grow in Importance

How do you see the importance of identity management changing at your organization or agency over the next five years, if at all?

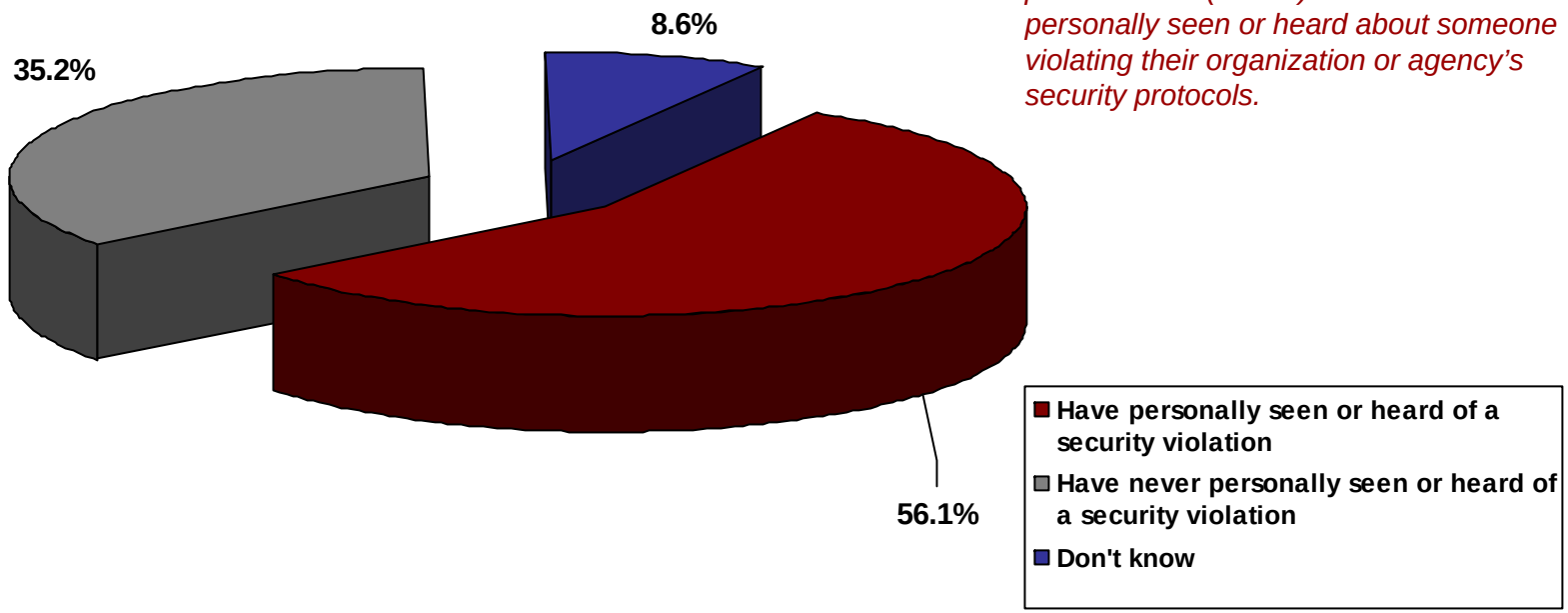


Most government IT professionals (71.7%) believe identity management will be "more important" over the next five years at their organization or agency.

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

More Than Half of Government IT Professionals Have Seen or Heard of a Violation to Security Protocols

Have you personally ever witnessed anyone violate your organization or agency's security protocols?

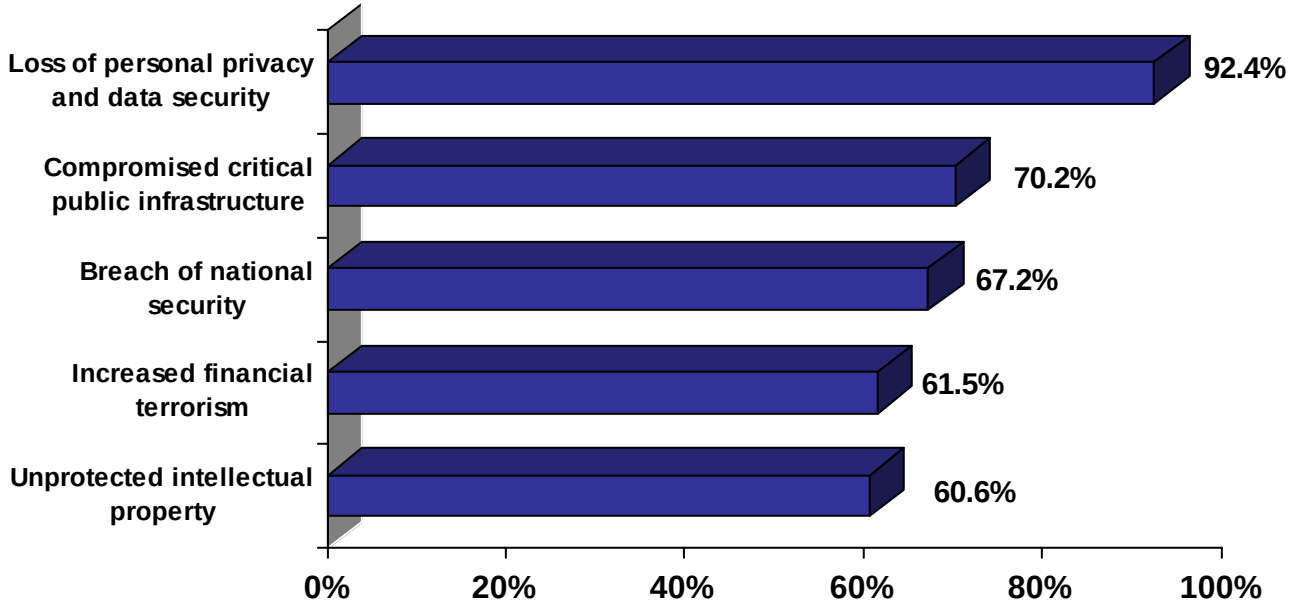


Over one-half of government IT professionals (56.1%) have either personally seen or heard about someone violating their organization or agency's security protocols.

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

Government IT Professionals Most Concerned with Loss of Personal Privacy/Data Security if Unauthorized Parties Access Their Network

For each of the following, if the information your organization or agency houses on your network was acquired by unauthorized parties, how concerned would you be that the following could occur?



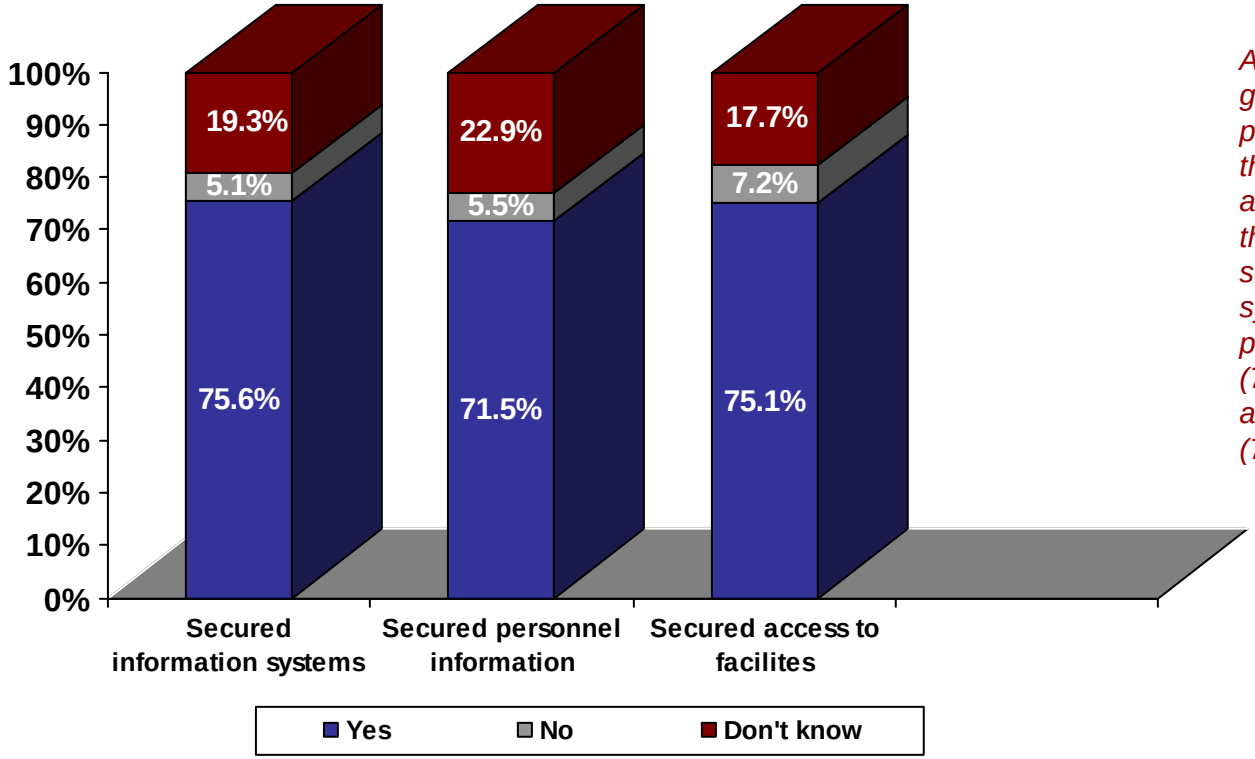
Total Concerned ("Very concerned" or "Somewhat concerned")

Nine in ten (92.4%) government IT professionals would be concerned about the loss of personal privacy and data security if unauthorized parties were to access information on their organization or agency's network.

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

A Large Majority Believe Their Org./Agency Has Already Taken Many Steps Toward IdM Compliance

Please indicate whether your organization or agency has taken each of the following steps to comply with HSPD-12, FIPS 201, FISMA and other identity management-related mandates?

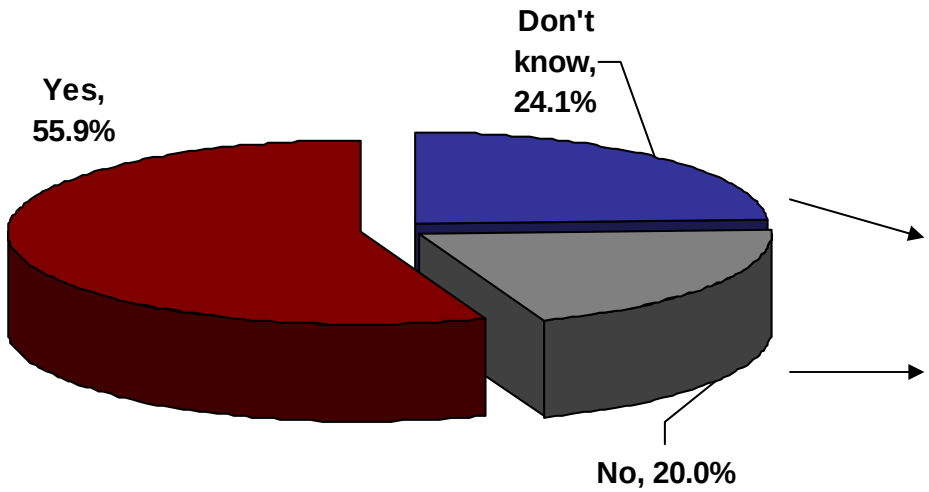


A large majority of government IT professionals report that their organization or agency has complied with the following steps: secured information systems (75.6%), secured personnel information (71.5%), and secured access to facilities (75.1%).

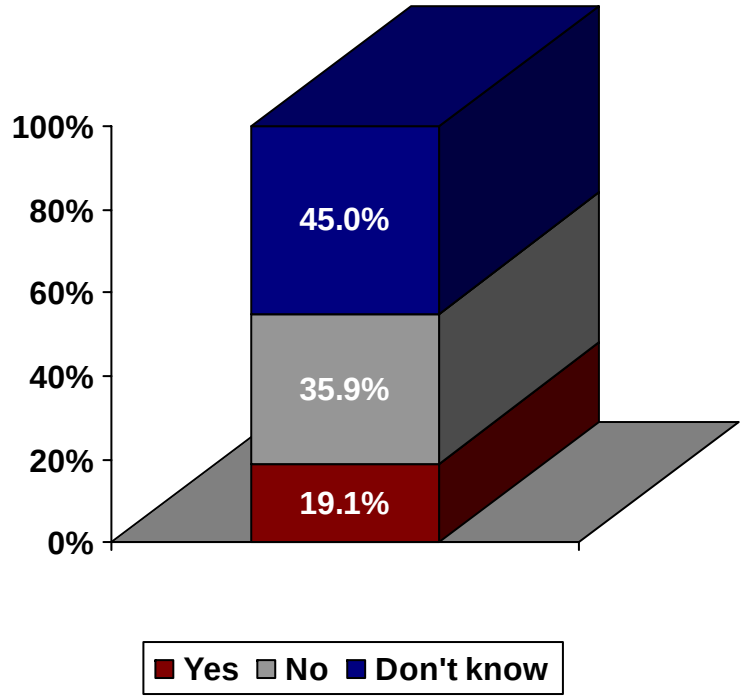
QUEST SOFTWARE® PUBLIC SECTOR
Government & Education Solutions

A Majority Say their Org./Agency Is Instituting an IdM System; 20% Have One Already in Place

Is your organization or agency currently instituting an identity management system?



Does your organization or agency already have an identity management system?

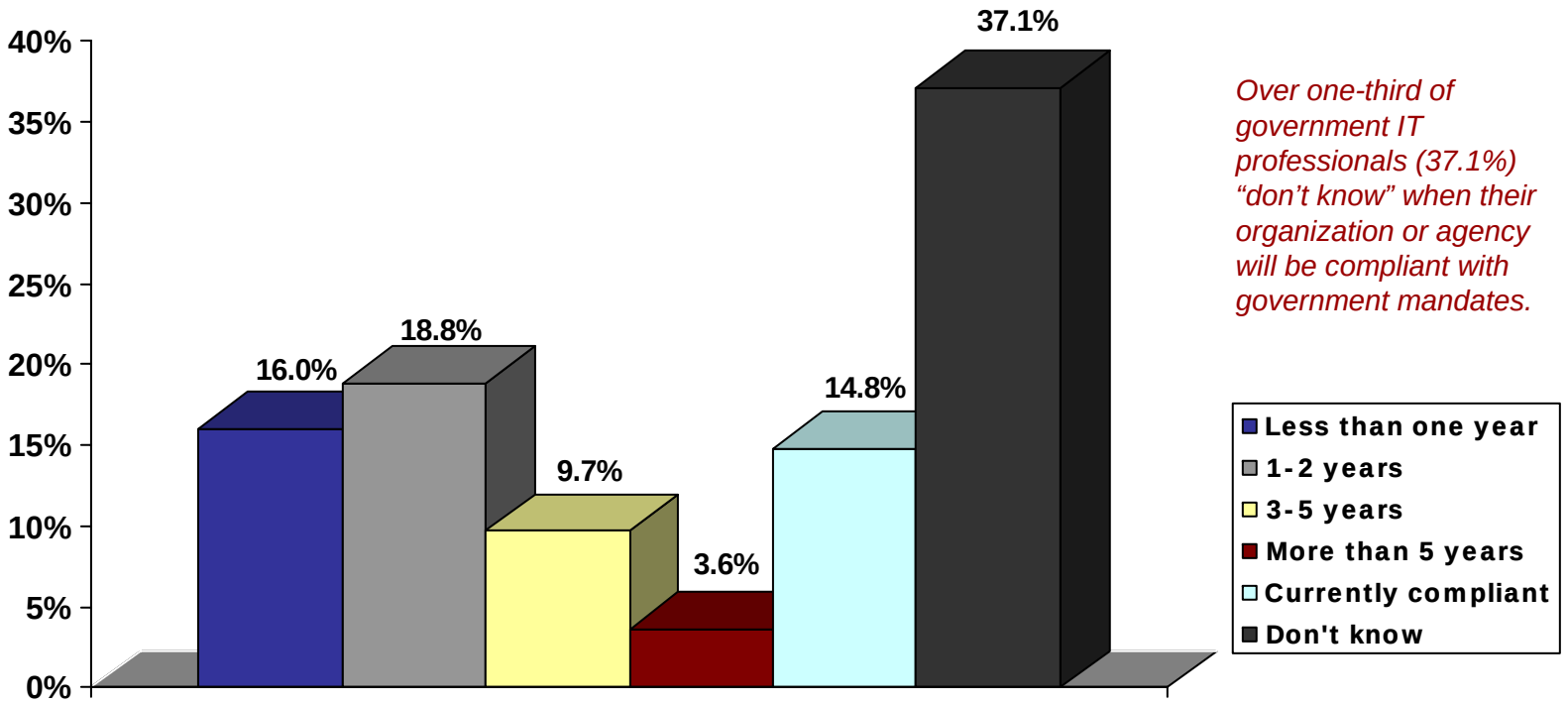


Over one-half (55.9%) state their organization or agency is instituting an identity management system, and another 19.1% state there is already one in place.

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

A Plurality "Don't Know" When Their Org./Agency Will Be Compliant with Federal IdM Mandates

When do you project your organization or agency will be compliant with identity management mandates like HSPD-12, FIPS 201, FISMA, etc.?



Over one-third of government IT professionals (37.1%) "don't know" when their organization or agency will be compliant with government mandates.

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

Lack of Funding Main Obstacle to IdM Objectives, Insufficient Staffing, Technological Complexity Follows

*In your opinion, which of the following **most** impacts your organization or agency's ability to reach its identity management objectives?*

Obstacles	**%**
Lack of funding	30.8%
Insufficient staffing resources	18.8%
Technological complexity	18.1%
Lack of knowledge base to deal with operational or technical issues	13.5%
Lack of management support and direction	11.8%
Other/Don't know/refused/none	7.0%

Lack of funding was stated by one-third of government IT professionals as an obstacle to their organization or agency when trying to attain its identity management objectives.

Congress Should Provide More Funding, Require Greater Collaboration and Planning in IdM

*Which describes the role, if any, you believe Congress should play in identity management? Check all that apply. **

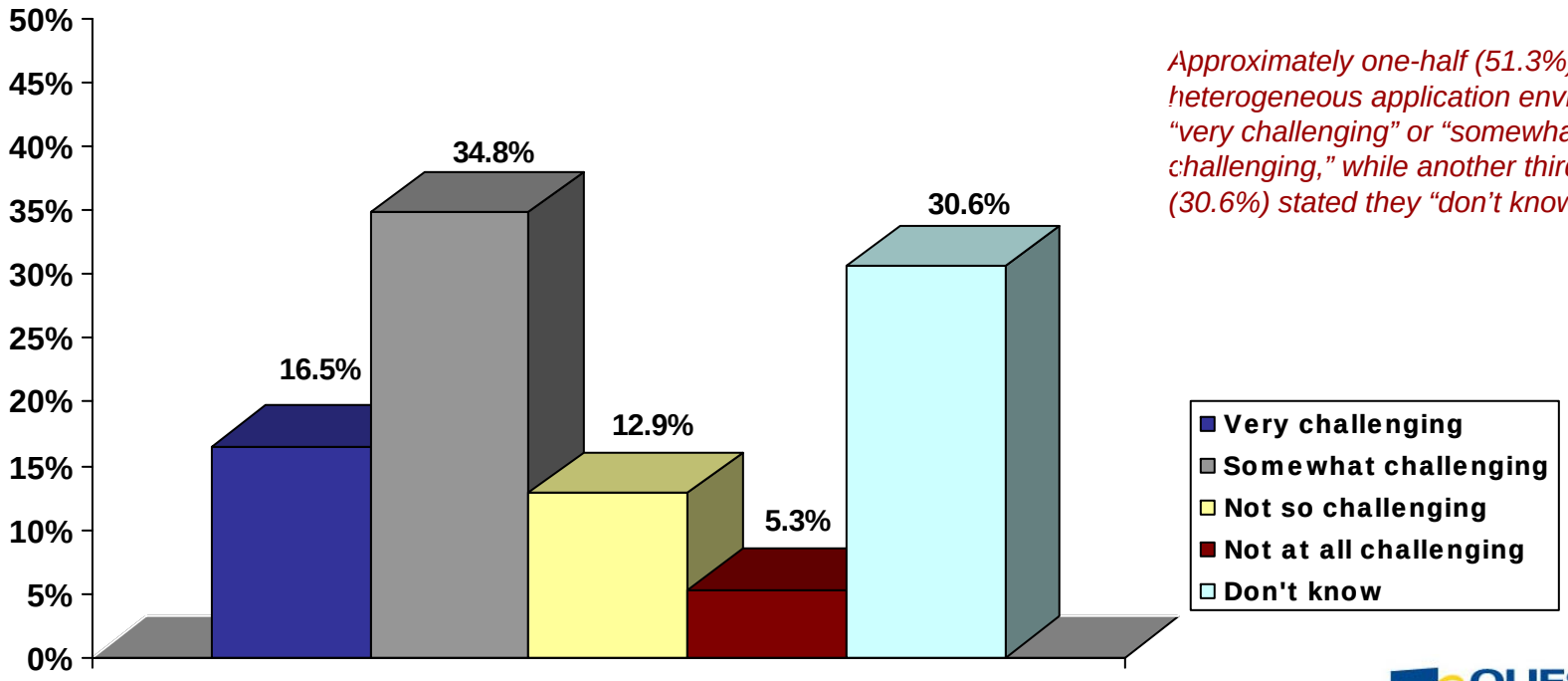
Role	%
Provide more funding to agencies to develop and implement identity management systems	50.4%
Require greater identity management planning and collaboration among federal agencies and state and local governments	48.9%
Provide greater oversight to assure agencies have effective identity management plans	29.7%
Congress should not have a role	11.4%
Direct the identity management effort	7.2%
Don't know	6.3%

While few government IT professionals believe Congress should direct the effort (7.2%), one-half state Congress should provide more funding (50.4%) and/or require greater collaboration between federal, state and local entities (48.9%).

*Respondents were able to select multiple responses. Percentages add to more than 100%.

Heterogeneous Application Environment Poses Challenges for a Majority in Single/Reduced Sign-on In IdM

How challenging is a heterogeneous application environment (e.g., Windows, Linux, Unix, Java) to single or reduced sign-on in identity management at your organization/or agency?

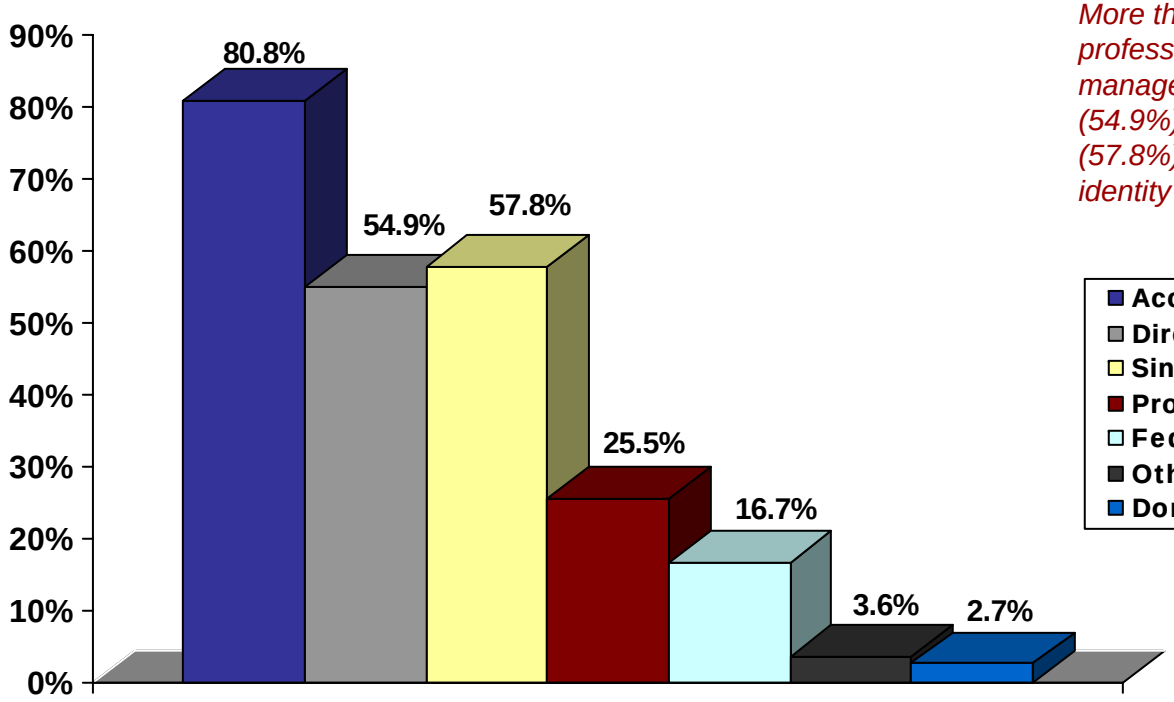


Approximately one-half (51.3%) find a heterogeneous application environment "very challenging" or "somewhat challenging," while another third (30.6%) stated they "don't know."

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

Access Management Leads Other Essential Components of IdM Systems, Followed by Single/Reduced Sign-on

*Which of the following are essential components of an identity management system? Please check all that apply.**



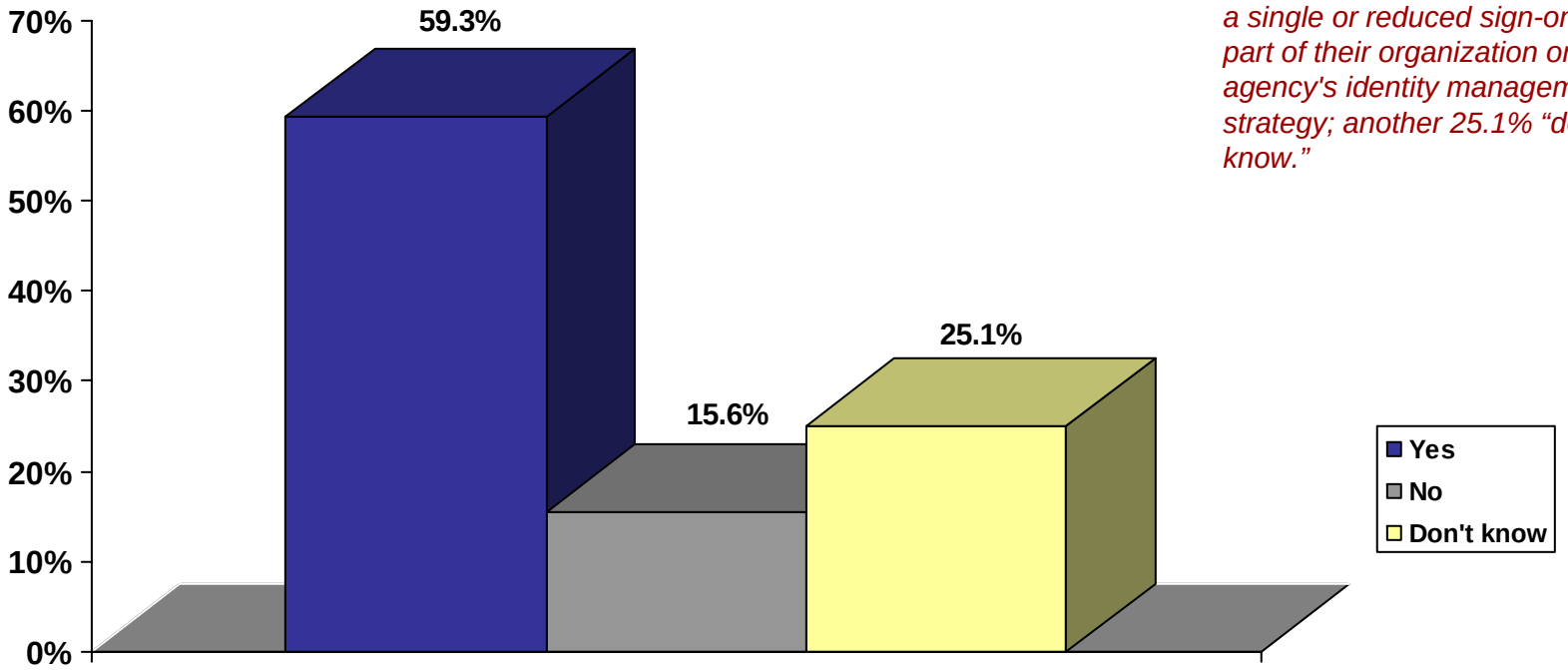
More than one-half of government IT professionals state that access management(80.8%), directory services (54.9%), and single/reduced sign-on (57.8%) are essential components of an identity management system.

*Respondents were able to select multiple responses. Percentages add to more than 100%.

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

Most Government IT Professionals Say Single or Reduced Sign-On a Part of Org./Agency's IdM Strategy

Is a single or reduced sign-on a part of your organization or agency's identity management strategy?

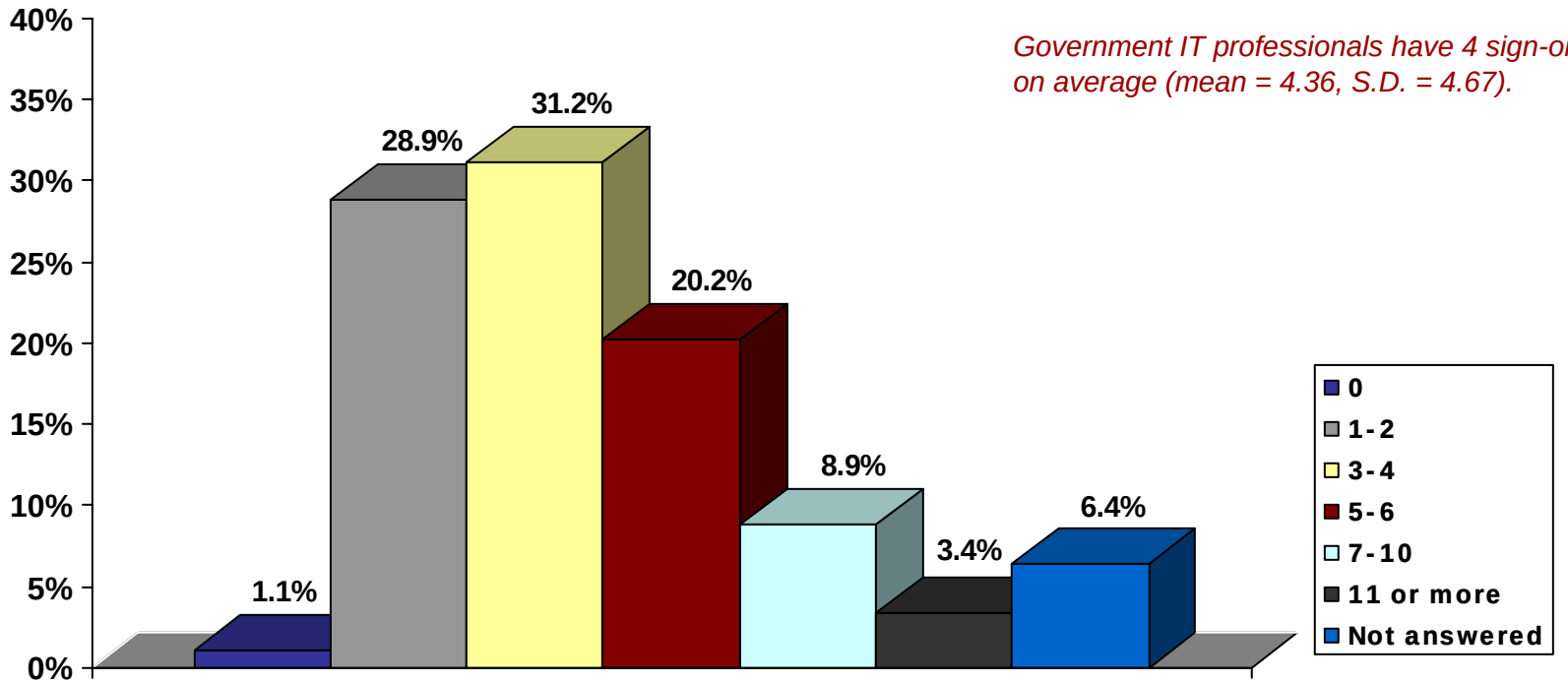


Sixty percent (59.3) report that a a single or reduced sign-on is a part of their organization or agency's identity management strategy; another 25.1% "don't know."

QUEST SOFTWARE PUBLIC SECTOR
Government & Education Solutions

Four Sign-ons the Average for Government IT Professionals; Nearly a Third Have 5 or More

*Currently, how many different sign-ons do you have to access the various systems and applications **you use daily**?*



Government IT professionals have 4 sign-ons, on average (mean = 4.36, S.D. = 4.67).

QUEST SOFTWARE
PUBLIC SECTOR
Government & Education Solutions

Summary

- HSPD-12 is about more than just the card...
- Critical links to an integrated identity management system:
  - **A**uthentication
  - **A**uthorization
  - **A**dministration
  - **C**ompliance
- Progress is being made. However, the complexity of IdM will grow exponentially, as the potential for compliance violations and security degradations increases.
- Public and private sector must continue to collaborate, as IdM grows in importance.
- Leveraging existing investments to centrally manage identities saves time, money and resources – key obstacles identified by survey respondents.
- The best IdM strategy generates short-term operational benefits, while maintains a long-term balance of security, efficiency and compliance.

Quest Software Puts Government Agencies on the Runway for Successful Identity Management

- While a utopian solution is far off, government agencies cannot afford to wait for the next disaster to occur.
- Technology exists today that leverages existing IT investments that can remedy significant concerns in protecting the integrity of the U.S. government's critical infrastructure.
- One of the biggest barriers to achieving an integrated IdM system is that the vast majority of government infrastructures are heterogeneous – comprised of mixed applications and platforms - and this will never change.
- The most significant step that government agencies can take to develop an integrated IdM system is to leverage Microsoft Active Directory — the most ubiquitous investment made by government agencies — to create a centralized identity repository and immediately allows work towards single/reduced sign on.
- For the first time, government agencies can have a unified IdM platform across Microsoft and non-Microsoft IT environments.
- Quest Software provides the most secure, scalable and compliant infrastructure for authentication available today.

QUEST SOFTWARE®
PUBLIC SECTOR
Government & Education Solutions