



Federal Chief Information Security Officer Second Annual Survey Results

August 29, 2005

Contents

- Methodology
- Highlights
- Participant Background
- Help Desk Support
- Daily Duties
- Trend Report
- Product/Service Priorities
- Top Concerns
- Private Sector Considerations
- Wireless Security
- Observations

Methodology

- Intelligent Decisions conducted online and telephone interviews with 29 top-level government security professionals from both civilian and defense agencies
- Participant agency size varies from very small to very large (< 1,000 to > 50,000 employees)
- Purpose of the survey is to determine current and future information security priorities of Federal government executives, and to measure results against the Intelligent Decisions' First Annual Federal CISO study released in November 2004

Study Highlights

- The FISMA burden continues to grow, as Federal CISOs now spend an average of 3.75 hours per day on compliance activities
 - compared to 3.06 hours per day in the first study
- The top three trends Federal CISOs anticipate will increase over the next 12 months:
 - Increasing use of wireless networks and mobile devices
 - Single sign-on/multifactor authentication
 - Convergence of database and network security
- The top three products Federal CISOs consider most important to their agencies:
 - Network security/firewalls
 - Disaster recovery/continuity of operations planning
 - Authentication/PKI/encryption devices

Study Highlights Continued

- The top three activities Federal CISOs identify as most important for the private sector to consider:
 - Increasing software quality assurance
 - Developing a real-time FISMA compliance tool
 - Offer guaranteed levels of protection for managed security services
- The top three general security concerns of Federal CISOs:
 - Network compromise
 - Patch management
 - FISMA compliance
- The top three wireless security concerns of Federal CISOs:
 - Unauthorized wireless access points
 - Preventing unauthorized wireless deployments
 - Rogue WiFi devices

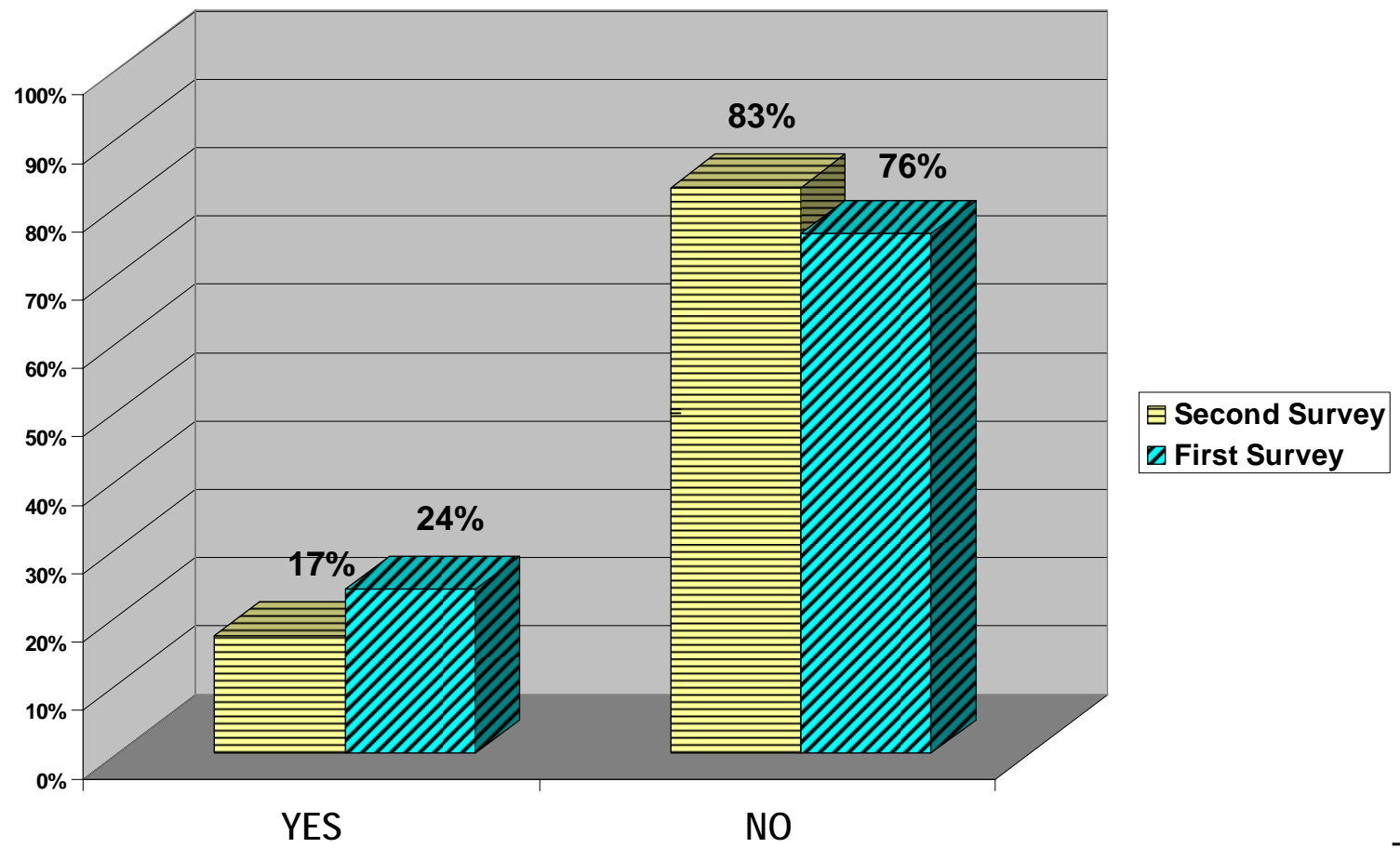


Participant Breakdown

<p>Years Served as Lead IT Security Role at Current Agency</p> <ul style="list-style-type: none">• Three or less = 50%• Three to five = 25%• Five to seven = 4%• Greater than seven = 21%	<p>Dedicated IT Security Professionals Managed</p> <ul style="list-style-type: none">• None = 14%• One to five = 43%• Five to 20 = 32%• Greater than 30 = 10%
<p>Annual technology budgets reflecting Capital Expense (CE) and Operation & Maintenance (O&M) averages of</p> <ul style="list-style-type: none">• CE = 39.23%• O&M = 60.76%	<p>Annual Technology Budget Responsibilities</p> <ul style="list-style-type: none">• Less than \$500,000 = 54%• Between \$500,000 & \$1 million = 7%• Between \$1 & \$5 million = 32%• Greater than \$10 million = 7%

Help Desk Support

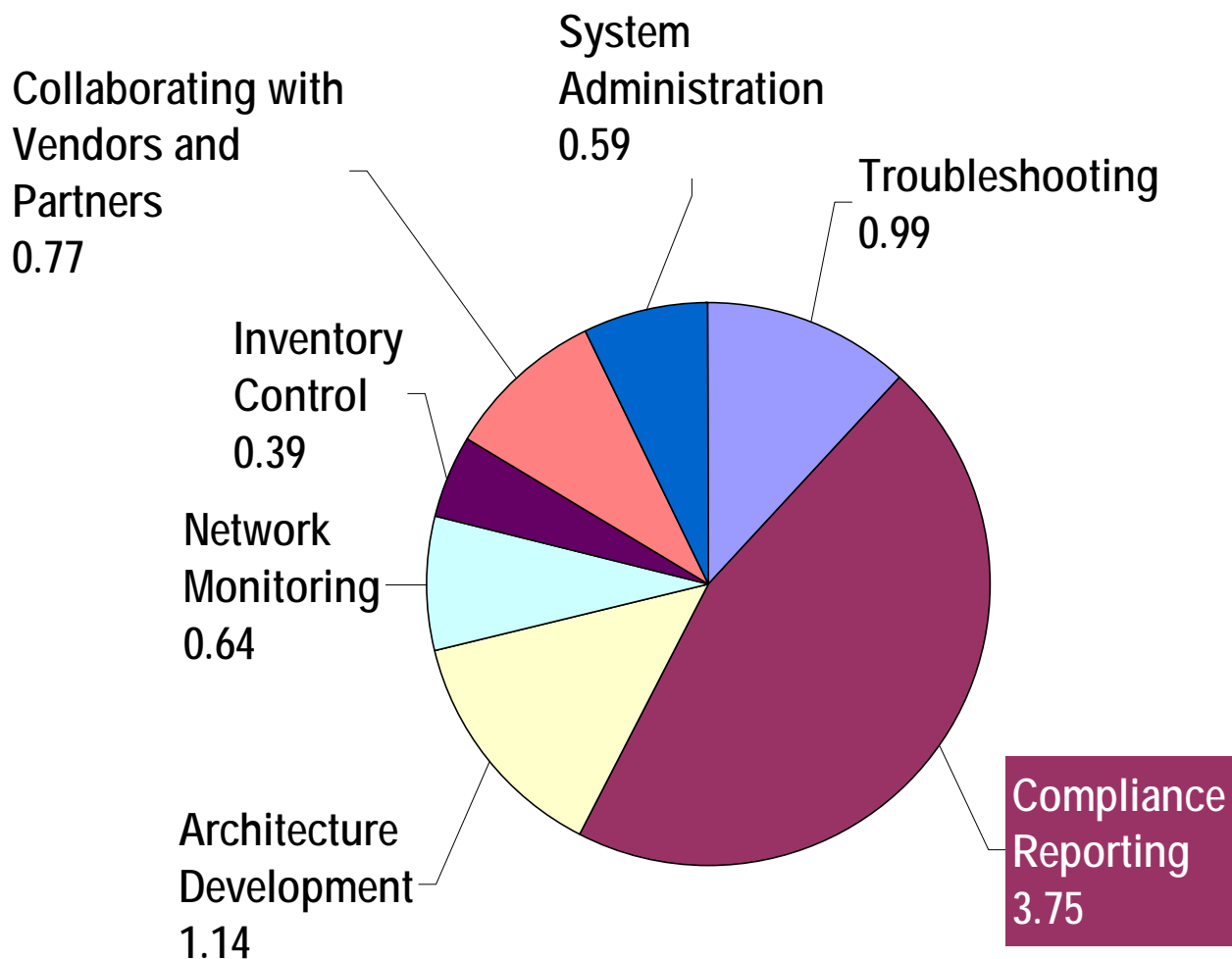
Does your agency have a help desk completely dedicated to IT security?





Daily Duties

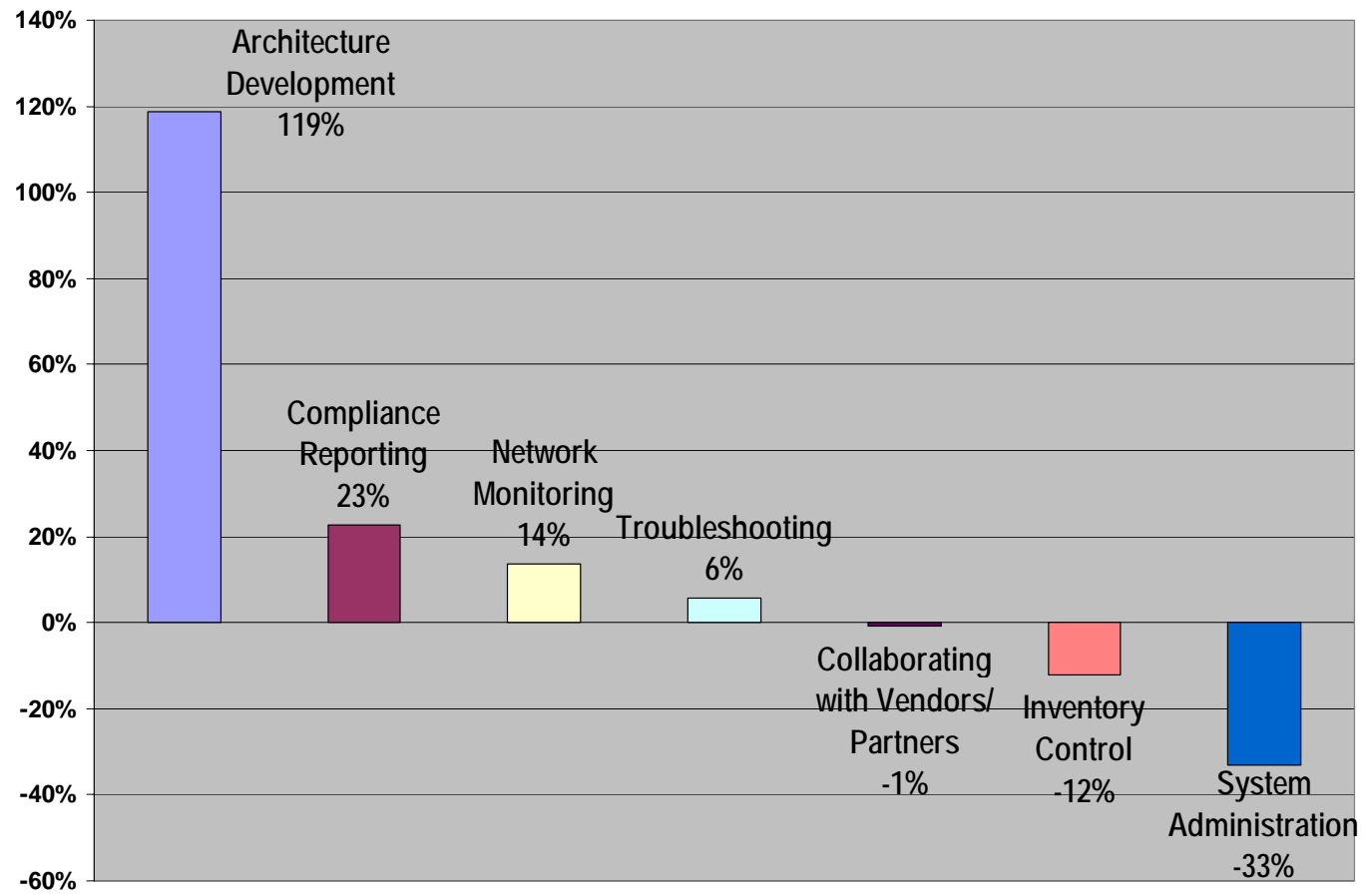
In a typical day, how many hours do you spend on the following tasks?





Daily Duties – Percent Change

Percent change in the average number of hours spent per task, Second Survey vs. First Survey

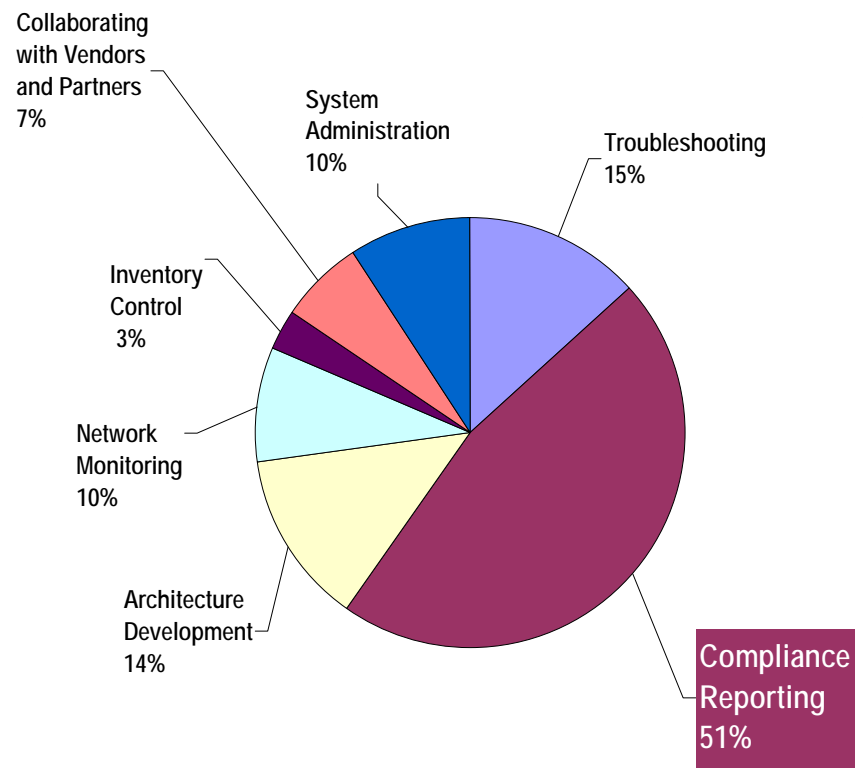




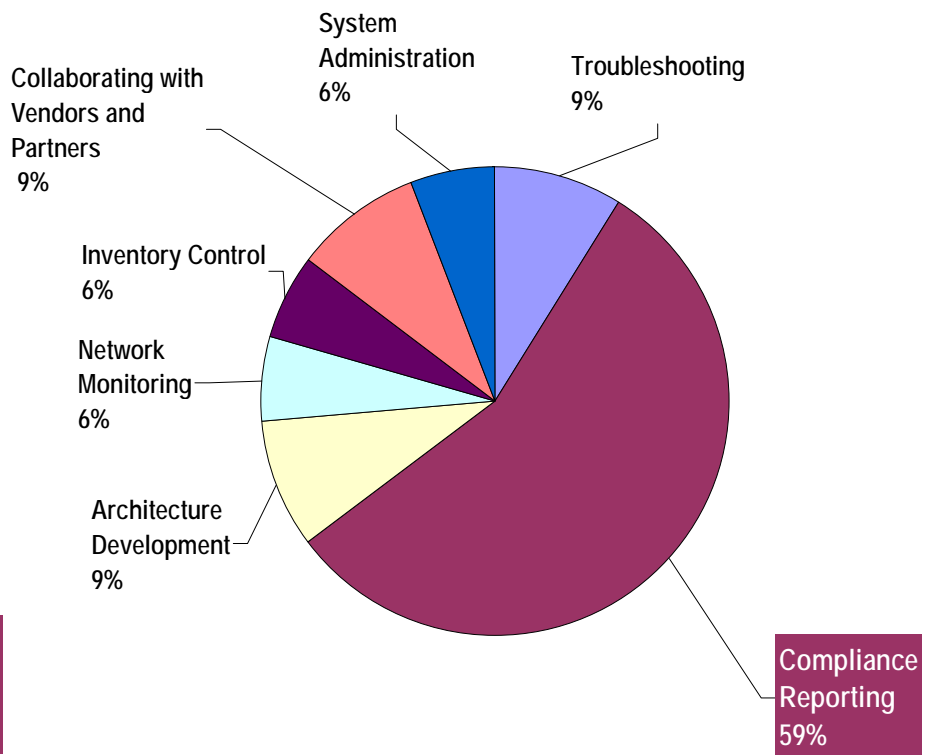
Daily Duties – Budget Authority

Percentage of time spent per task according to Federal CISO budget authority

< \$500,000

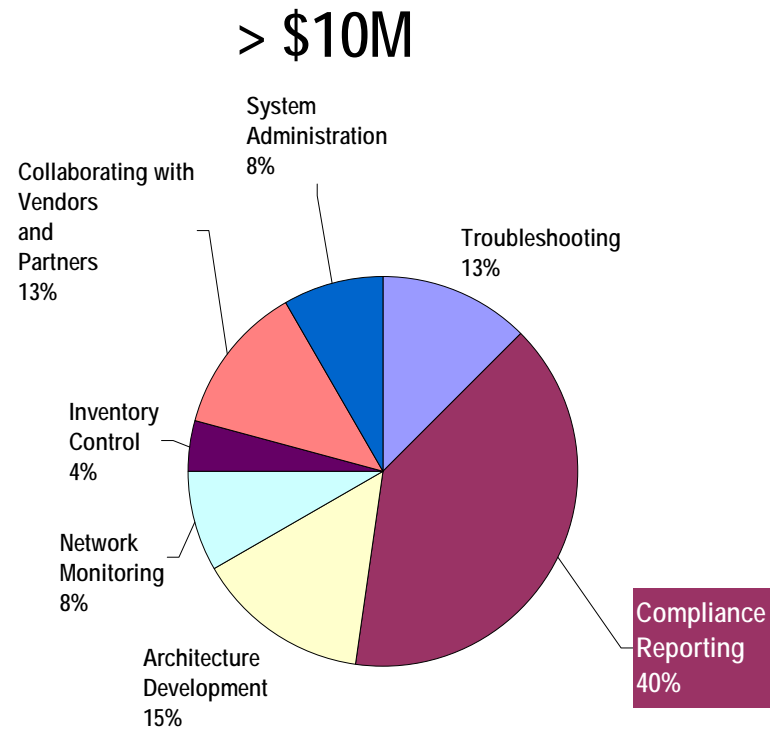
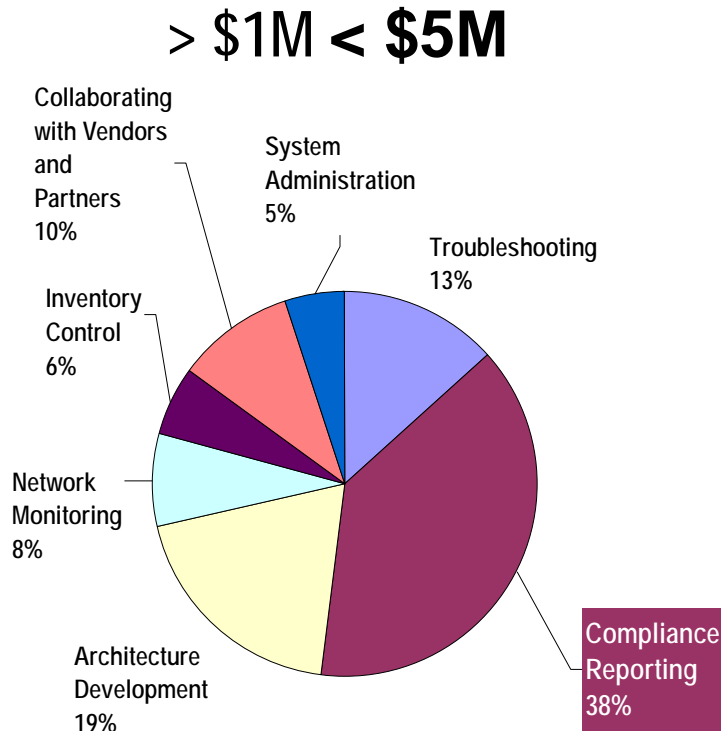


> \$500,000 < \$1M



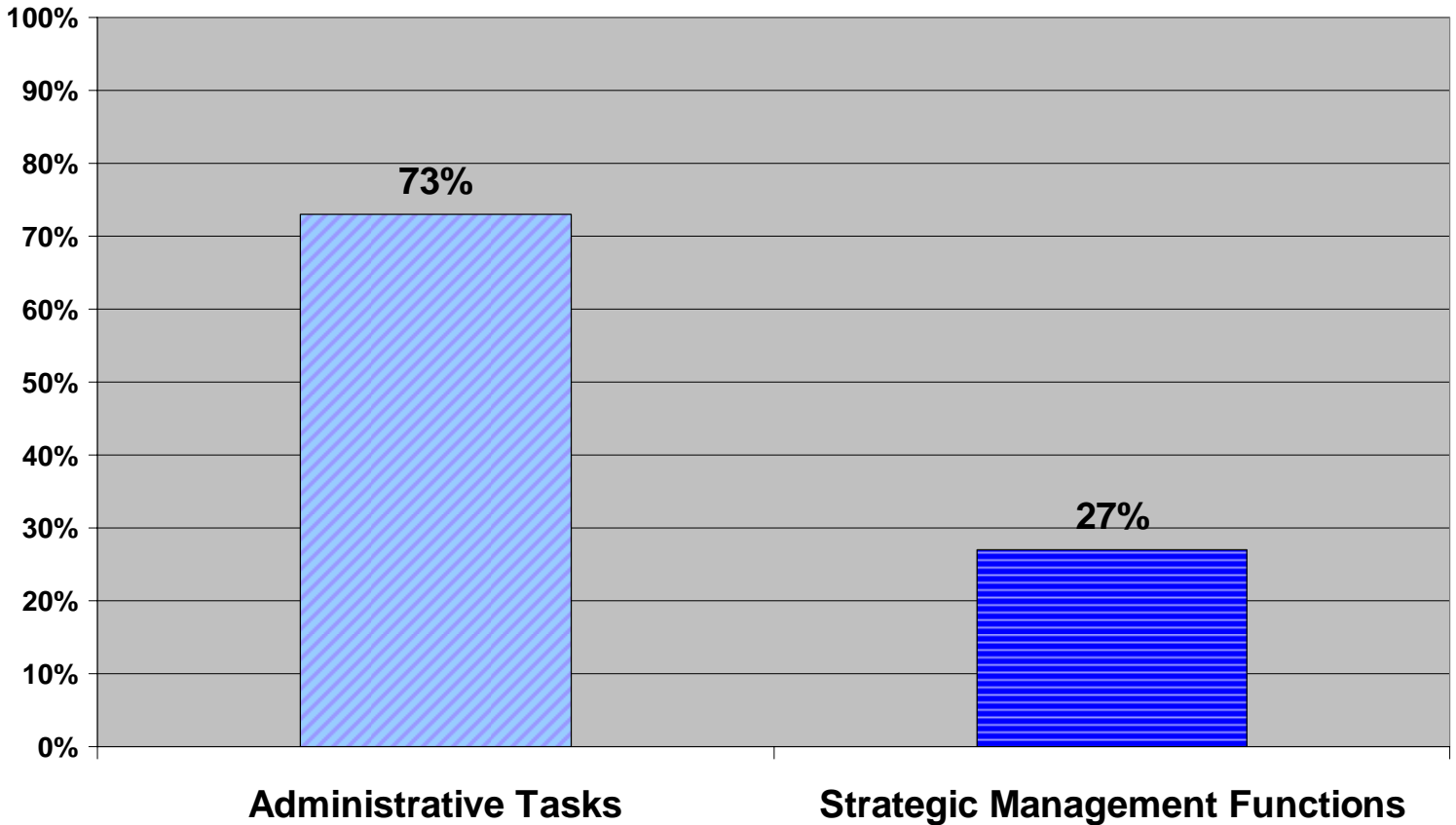
Daily Duties –Budget Authority continued

Percentage of time spent per task by Federal CISO budget authority



Daily Duties – Administrative vs. Strategic

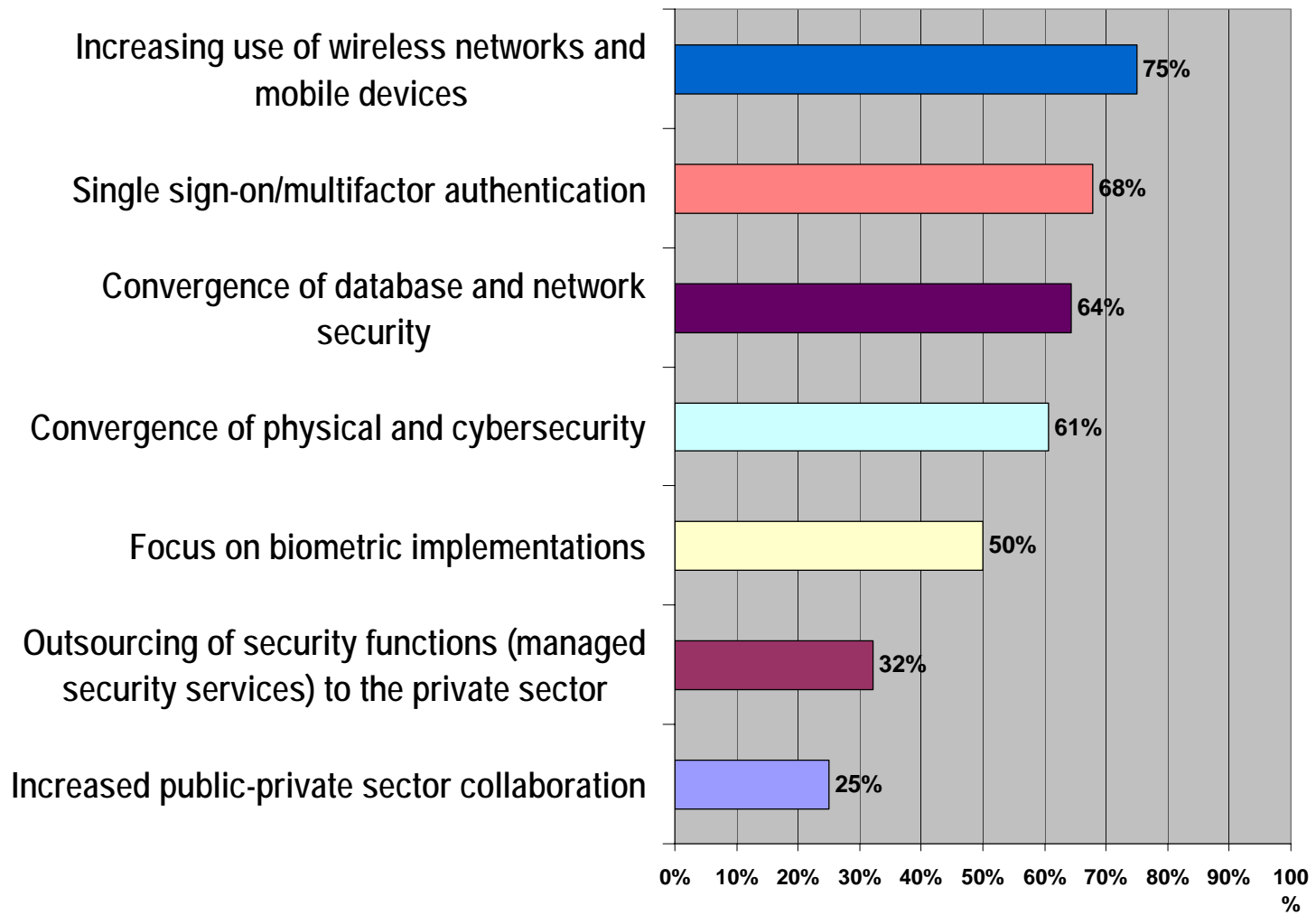
Percent time spent on administrative vs. strategic management functions





Trend Report

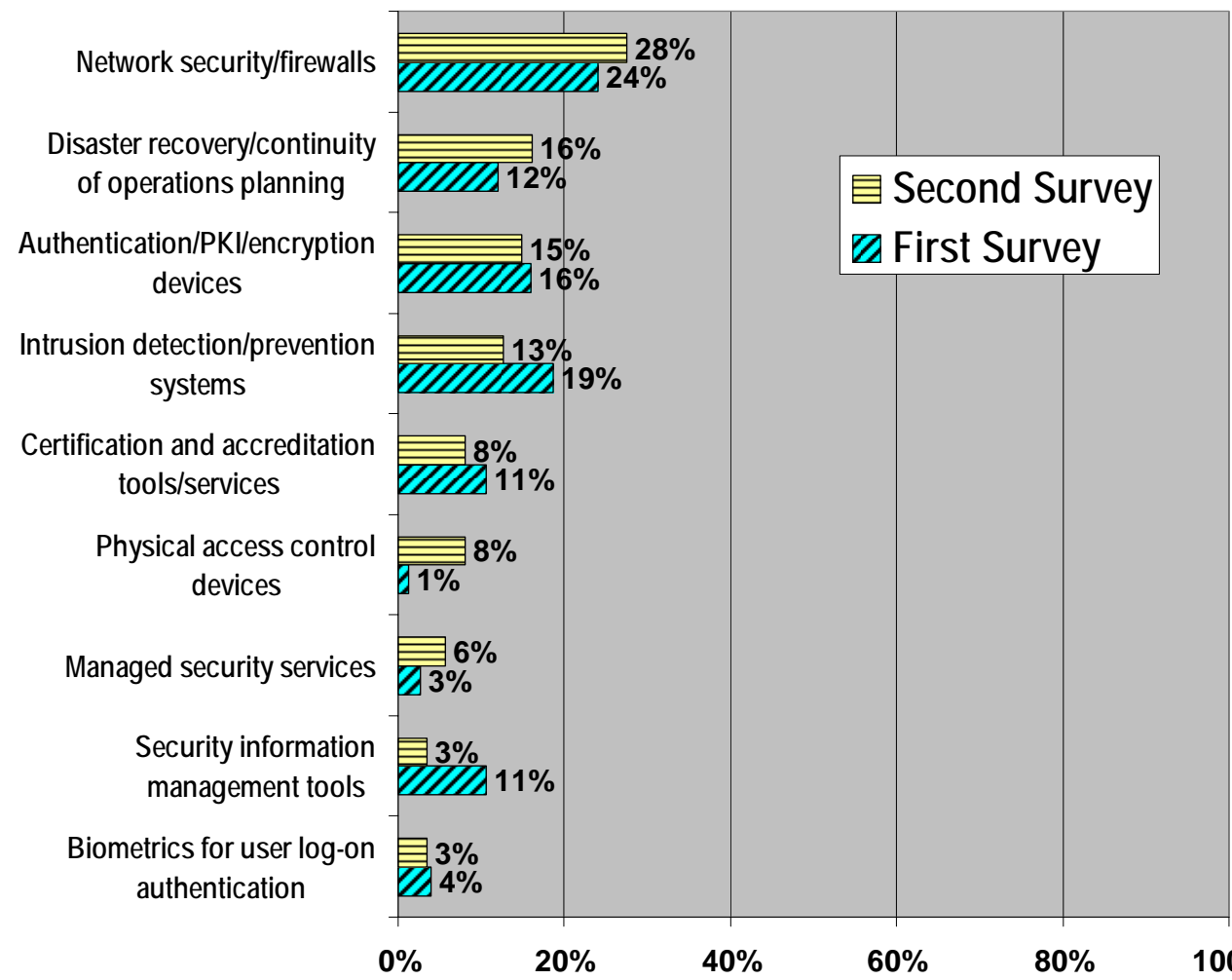
What trends do you anticipate will continue to increase momentum over the next 12 months?





Product/Service Priorities

What three products/services do you consider the most important to your agency?



PRODUCT/SERVICE	INDIVIDUAL RESPONSES SECOND SURVEY
Network security /firewalls	24
Disaster recovery/continuity of operations planning	14
Authentication/PKI/encryption devices	13
Intrusion detection/prevention systems	11
Physical access control devices	7
Certification and accreditation tools/services	7
Managed security services	5
Biometrics for user log-on authentication	3
Security information management tools	3

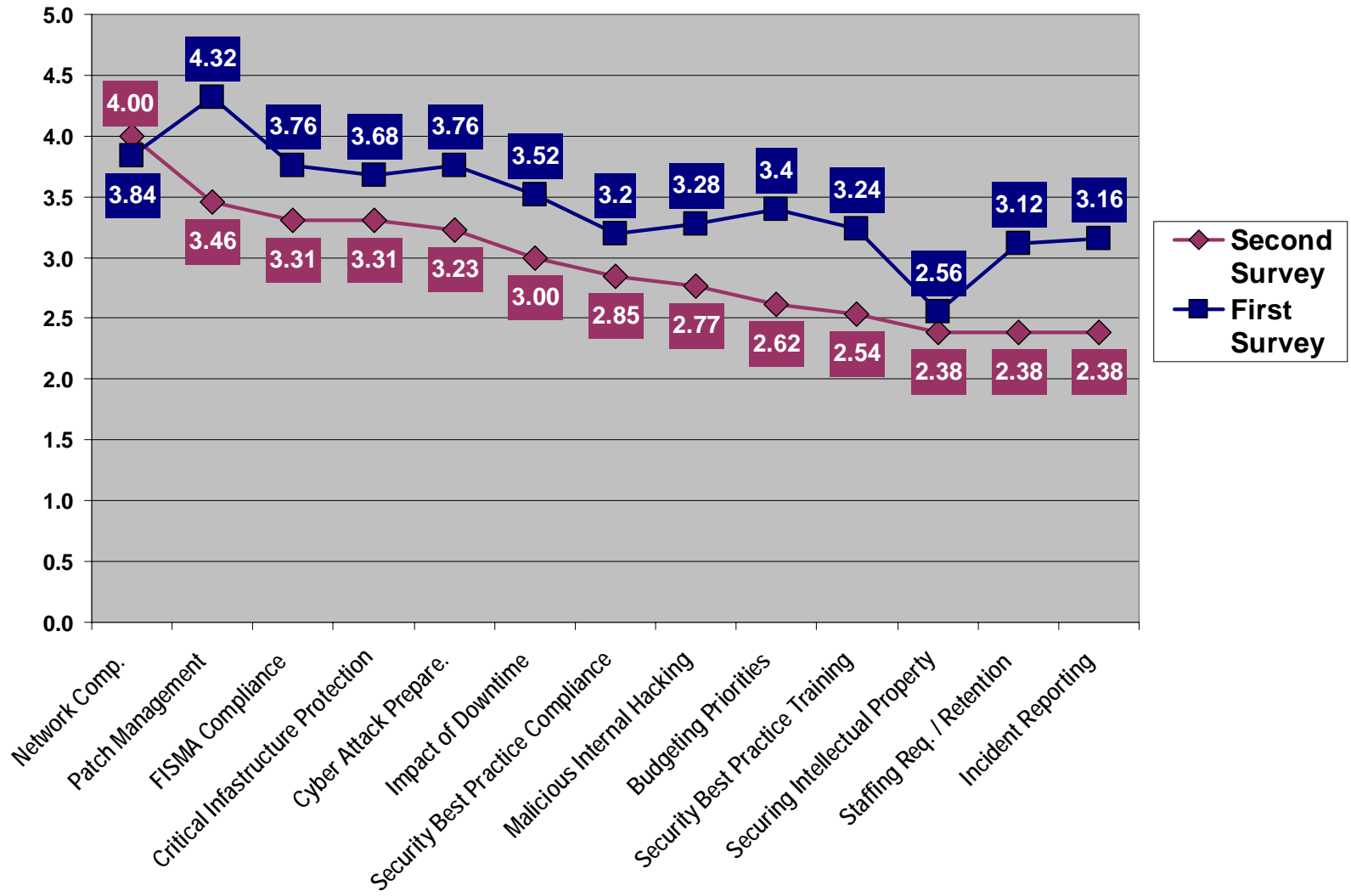


Top Concerns

Rank the following in terms of how much each is a concern to you.
(5 = highly concerned, 1 = not at all concerned)

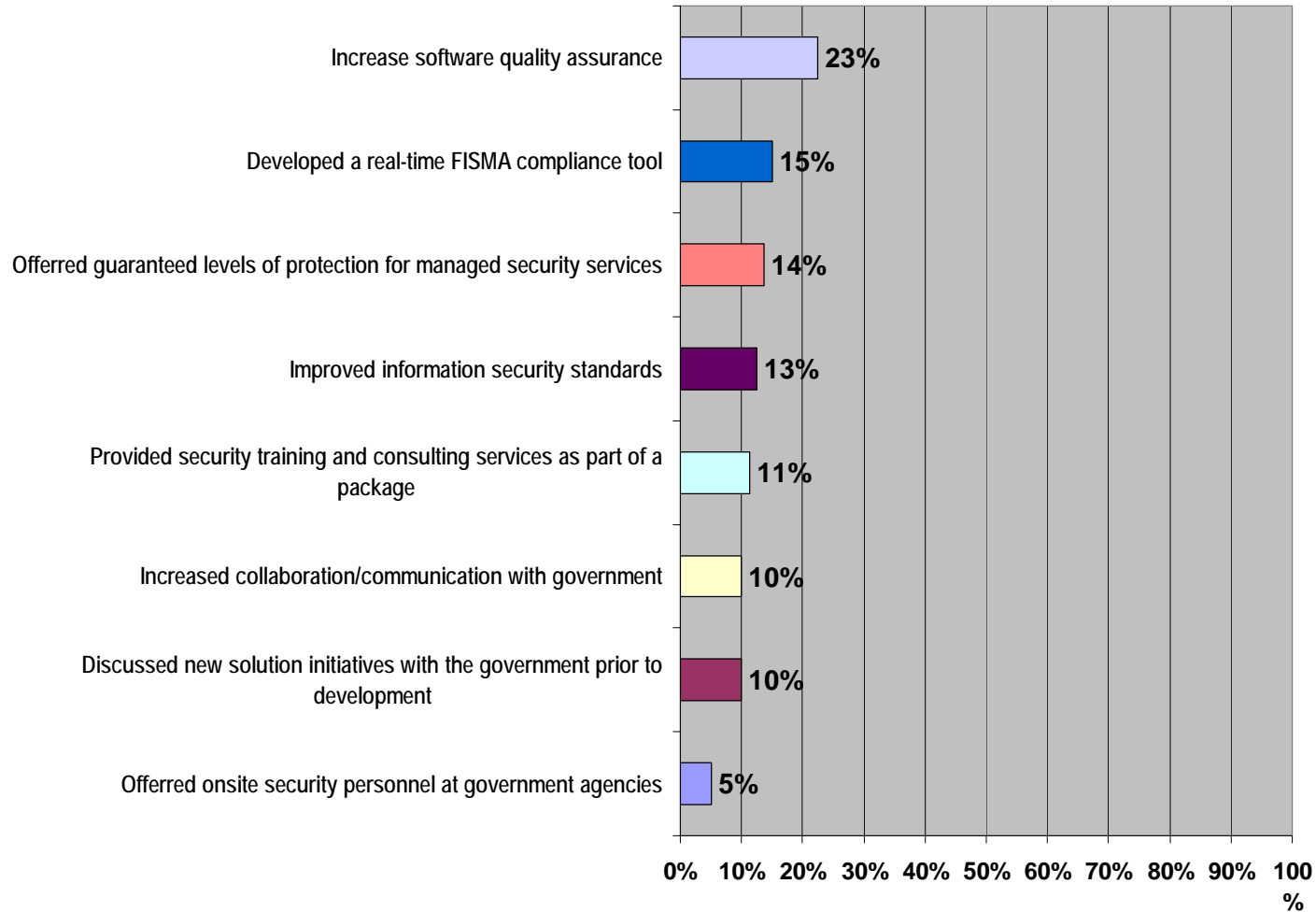
Network compromise	4	Malicious internal hacking	2.77
Patch management	3.46	Budgeting priorities	2.62
FISMA compliance	3.31	Security best practices training	2.54
Critical infrastructure Protection	3.31	Staffing requirements/ retention	2.38
Cyber attack preparedness	3.23	Incident reporting	2.38
Impact of downtime	3	Securing intellectual property	2.38
Security best practices compliance	2.85		

Top Concerns - Baseline Comparison



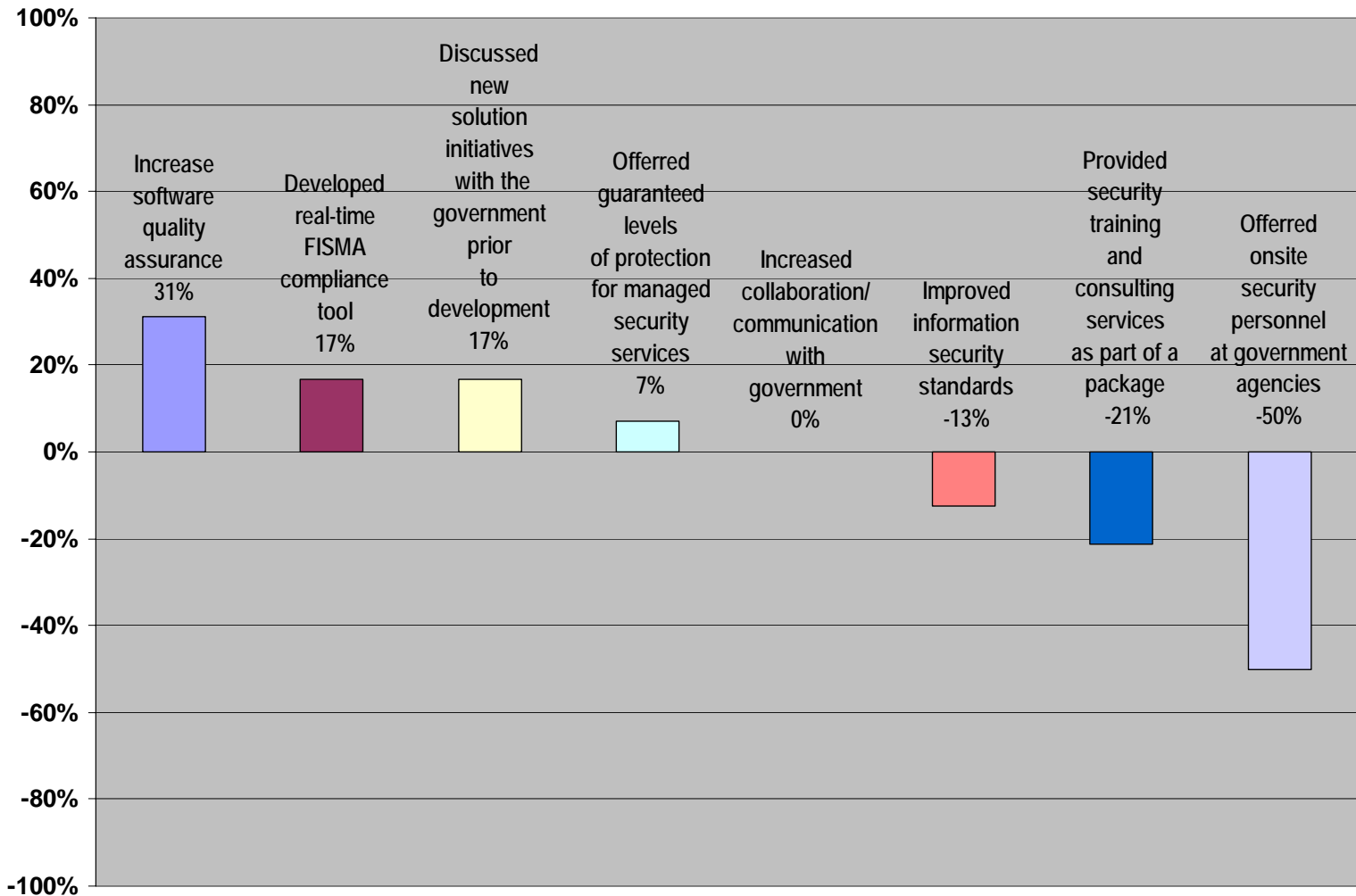
Private Sector Considerations

If the private sector did the following, which would you consider most important (select top 3)?



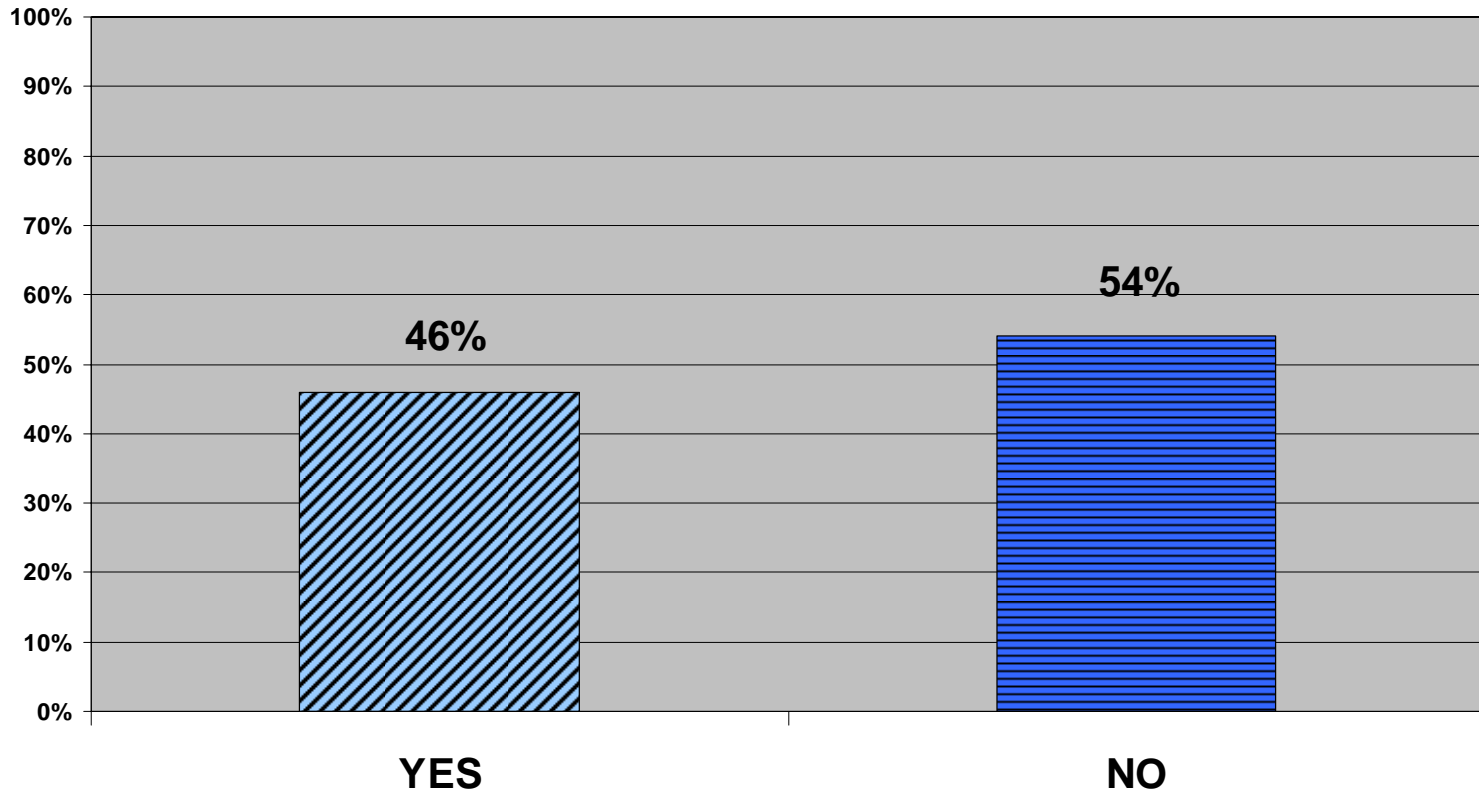
Private Sector Considerations – Percent Change

Percent change in the importance Federal CISOs assigned to private sector considerations, Second Survey vs. First Survey



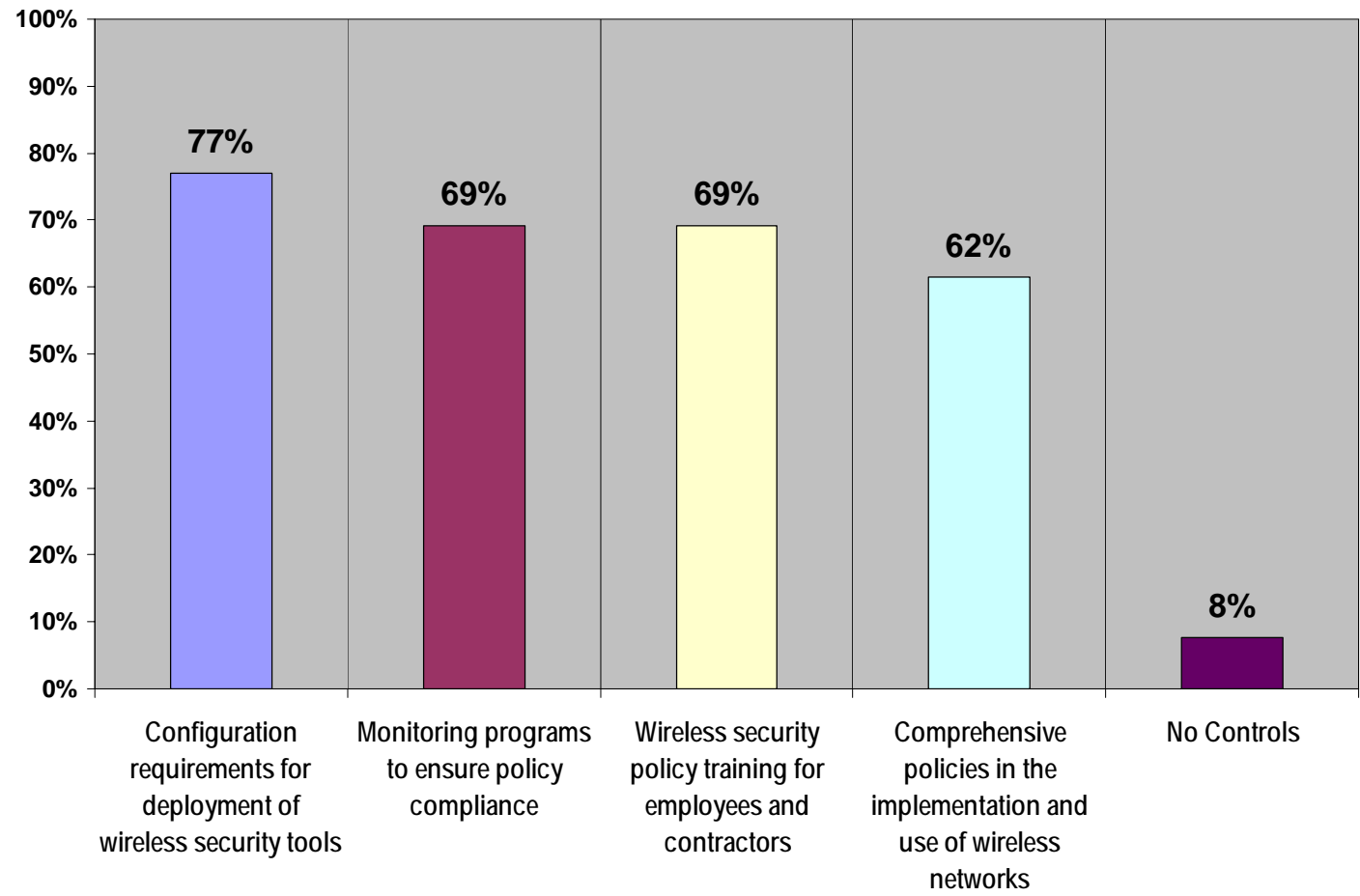
Wireless Security – Networks Maintained

Does your agency maintain wireless networks?



Wireless Security Controls

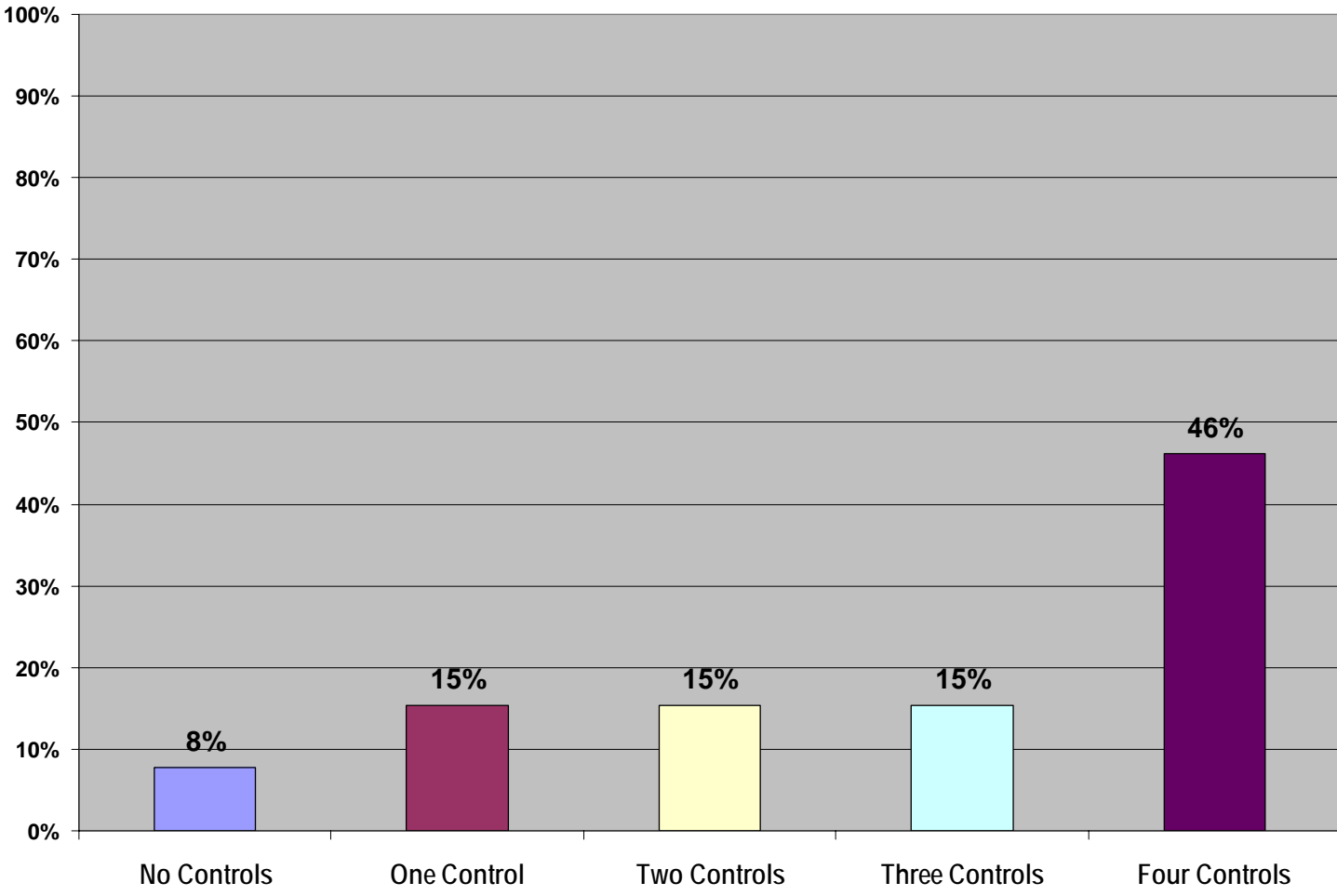
Which of the following basic security controls* has your agency implemented?



*See *Wireless Network Security: 802.11, Bluetooth and Handheld Devices (NIST Special Publication 800-48, November 2002)*

Wireless Security Controls – Implemented

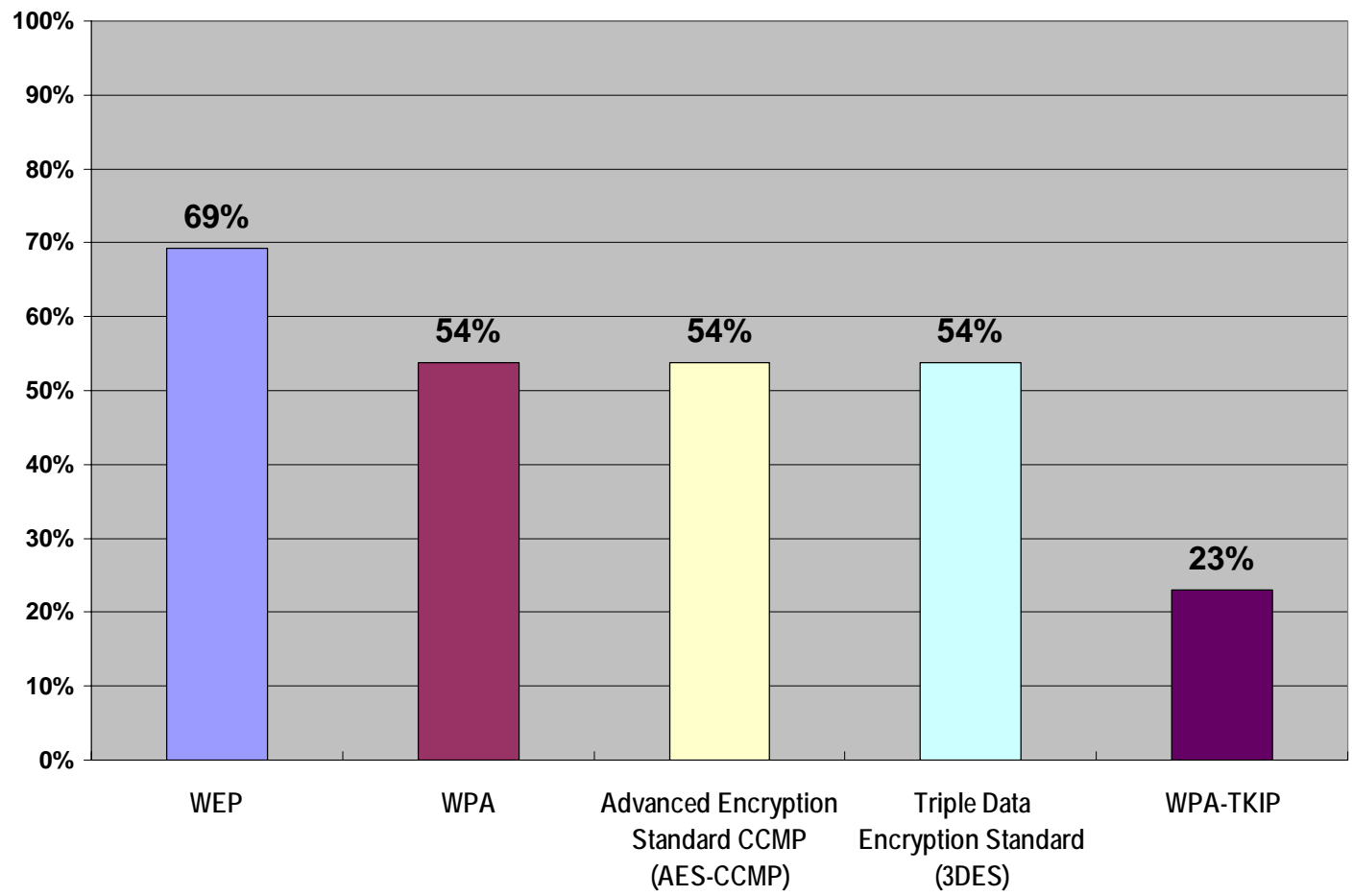
Percentage of the four basic wireless security controls Federal CISOs say their agency has implemented





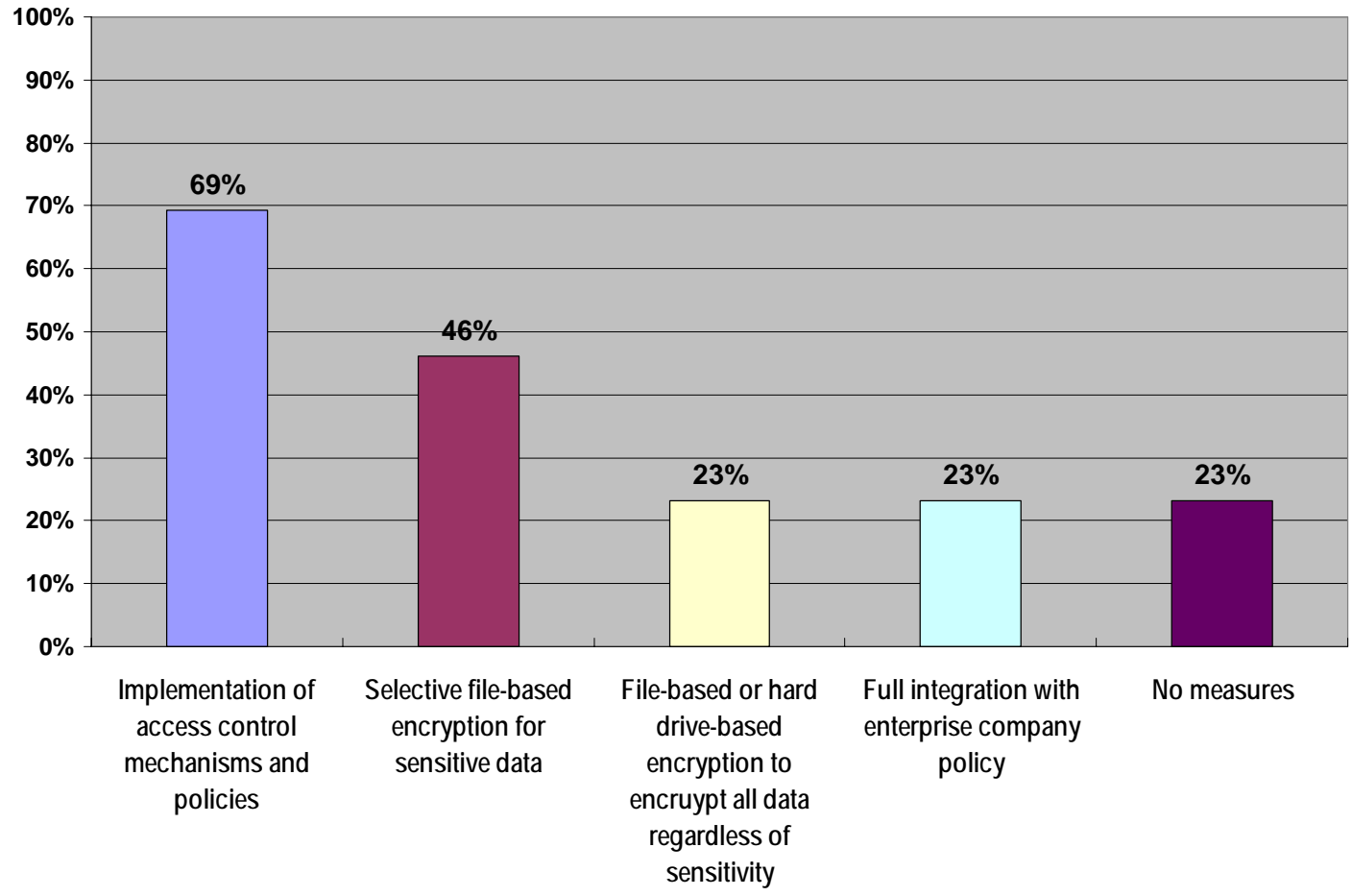
Wireless Security – Levels of Encryption

What level of encryption has your agency employed for securing access to wireless networks?



Wireless Security – Data at rest

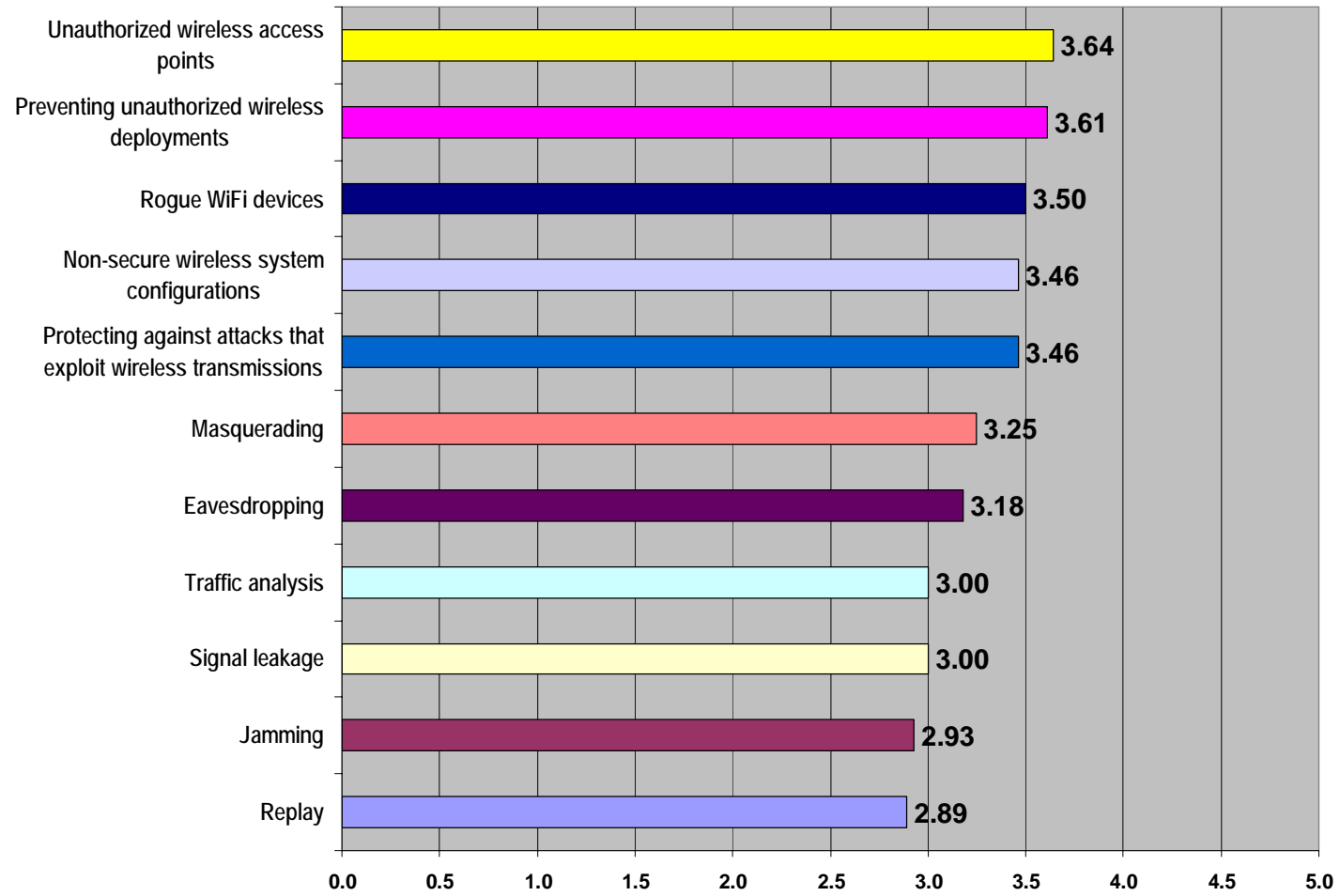
What measures has your agency taken to secure “data-at-rest” in handheld PDAs and smart phones using wireless networks?





Wireless Security – Top Concerns

Rank the following on how much each is a concern to you
(5 = highly concerned, 1 = not at all concerned)



Observations

- Federal CISOs consider increasing software quality and developing real-time FISMA compliance tools the top two areas on which industry needs to focus, suggesting that industry is not addressing CISOs most pressing concerns
- Federal CISOs are spending less time on system administration (-33 percent) and more time on architecture development (+119 percent), suggesting that Federal information security is becoming less of a technology problem and more of a policy and process development challenge
- Federal CISOs are spending significantly more time (+23 percent) on FISMA compliance reporting activities. Large agency CISOs are becoming just as challenged as small agency CISOs to carry out strategic management functions
- The scattered implementation of basic wireless security controls* suggests that the lack of guidance and mandatory requirements has led the majority of agencies to deploy wireless networks without taking complete steps to secure them from unauthorized access and other threats

*See *Wireless Network Security: 802.11, Bluetooth and Handheld Devices (NIST Special Publication 800-48, November 2002)*