CENTER FOR
INTERNET SECURITY®

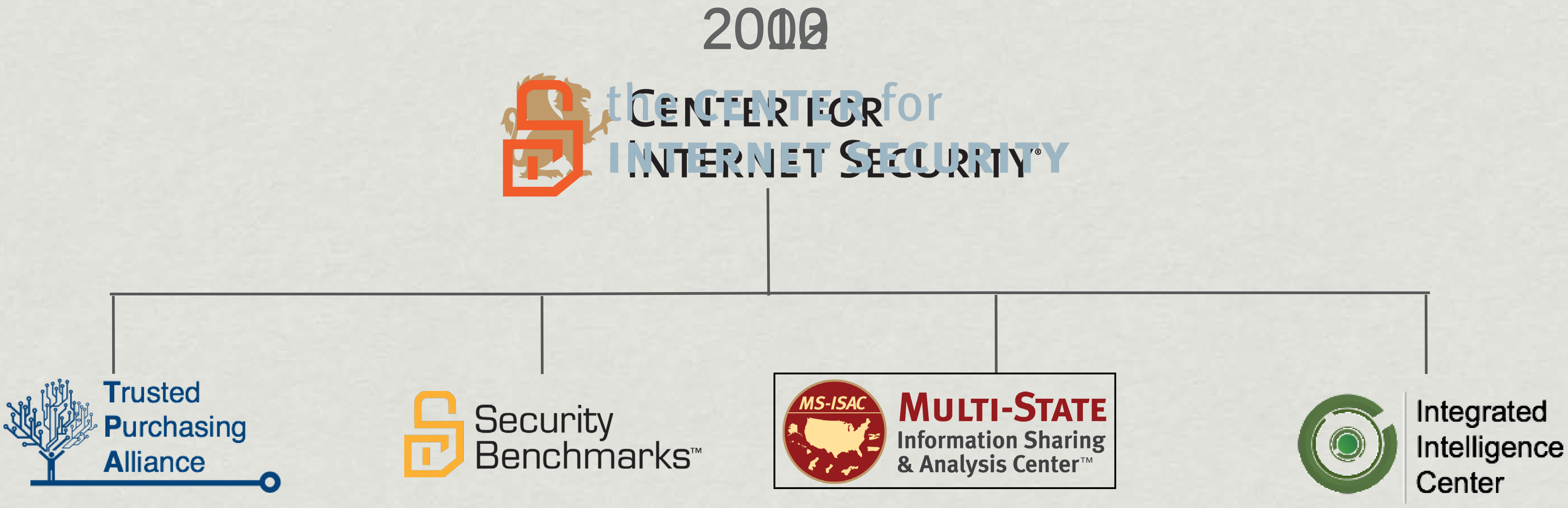
William F. Pelgrin
President and CEO

Posture of the Cyber Security Workforce in State, Local, Tribal and Territorial Governments

Asif Ismail
Program Manager
September 17, 2013

CIS and MS-ISAC Overview

CIS Organization Structure



2000

2012

the CENTER for INTERNET SECURITY

CENTER FOR INTERNET SECURITY®

Trusted Purchasing Alliance

Security Benchmarks™

MS-ISAC Multi-State Information Sharing & Analysis Center™

Integrated Intelligence Center

with Howard Schmidt
Former Cyber Security Coordinator
National Security Council
Executive Office of the President, White House
EXIT
EXIT
MULTI-STATE
Information Sharing
& Analysis Center
MS-ISAC
2012
Annual Meeting

MS-ISAC Members

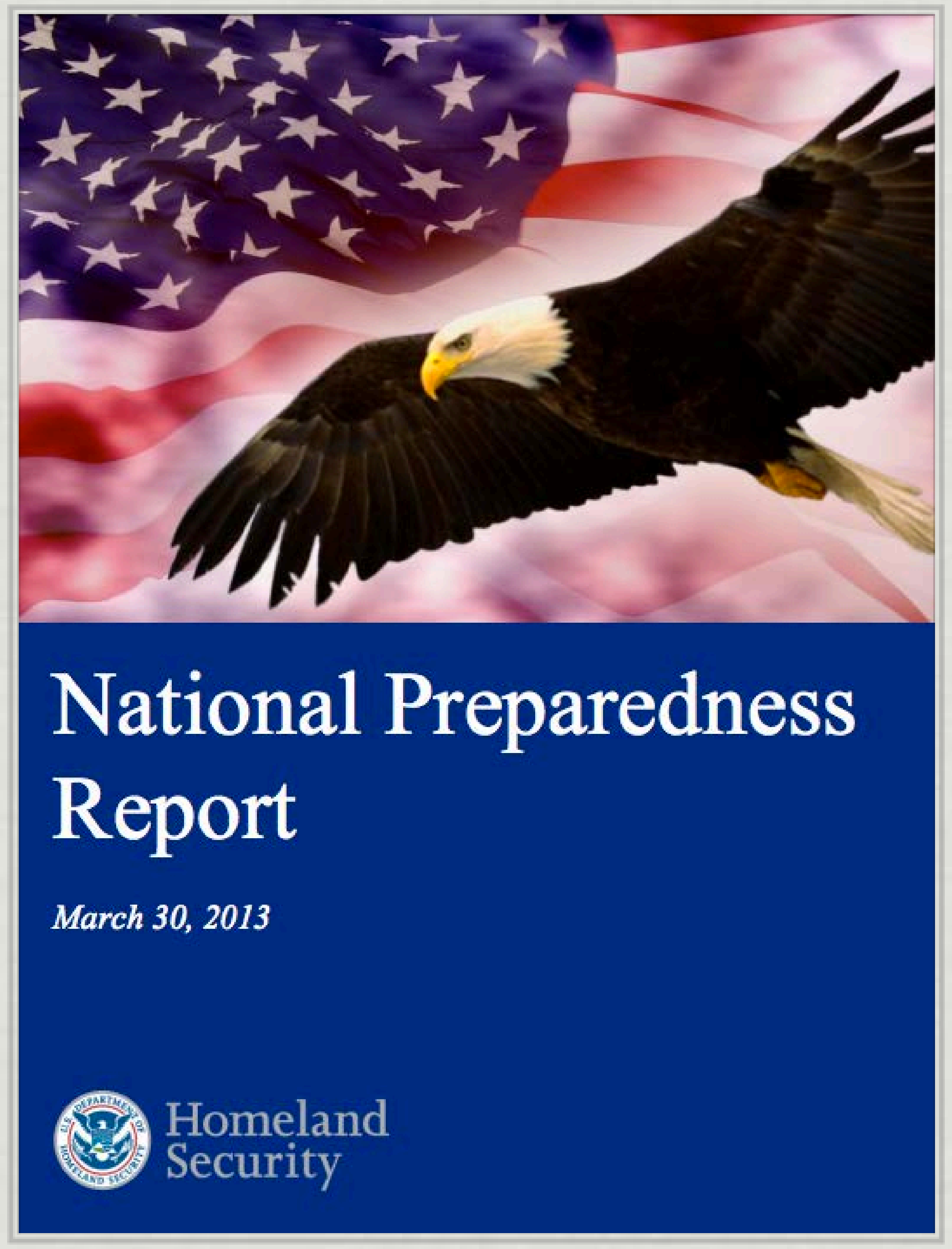
SLTT Sector and Cyber Security

The Problem

- The cyber security field is one of the fastest growing business sectors
  - Growth in new core competencies
- There is a shortage of skilled professionals
- There is a lack of funding and resources available to train the workforce

National Preparedness Report

- Describes the Nation’s approach to preparing for the threats and hazards that pose the greatest risk to the security of the United States.
- Assesses 31 core capabilities of all 50 States, D.C, and 5 Territories.



National Preparedness Report

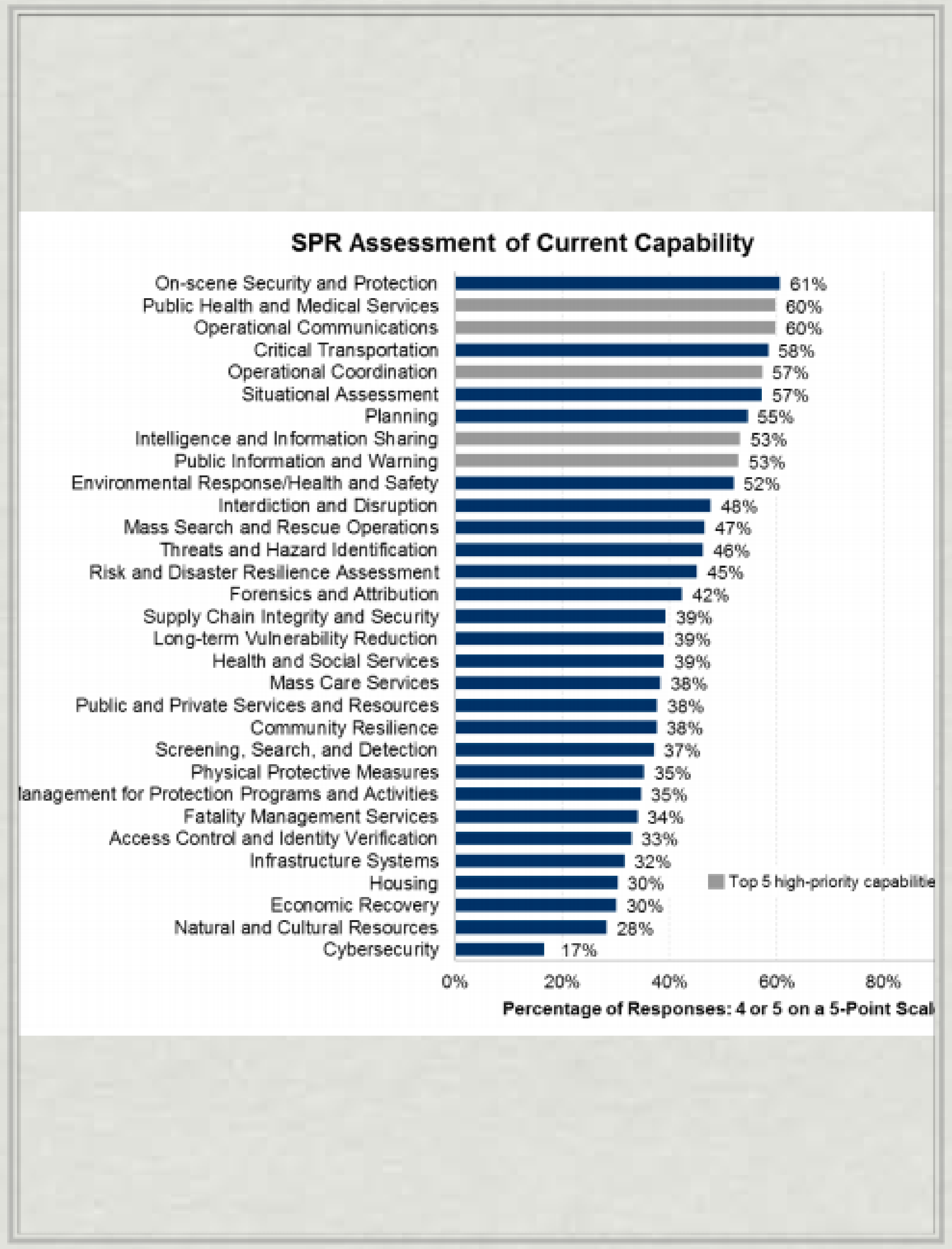
March 30, 2013

Homeland Security

National Preparedness Report

- Areas of strength: On-scene security and protection, public health and medical services, operational communications, critical transportation, operational coordination

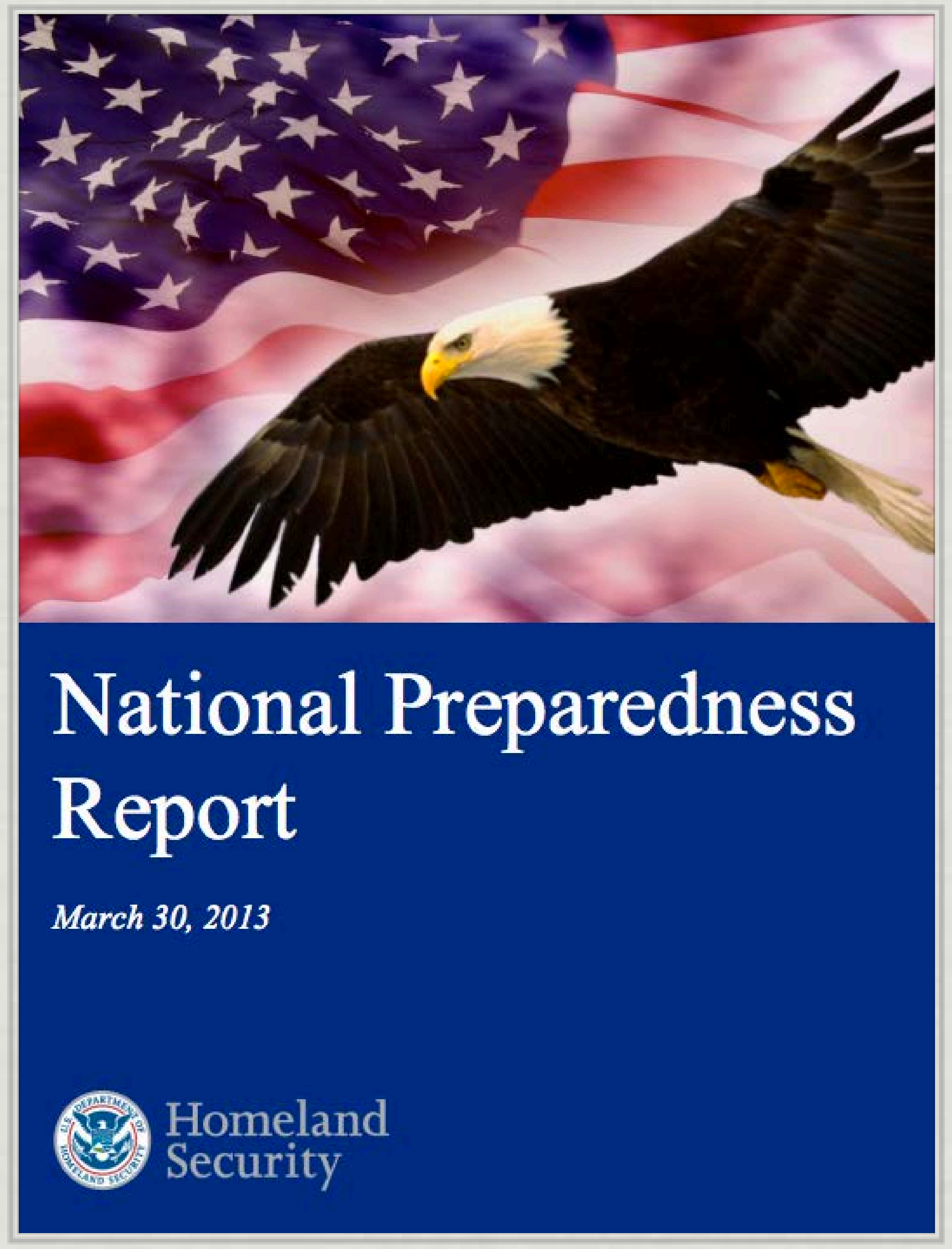
- Areas of weakness: natural and cultural resources, cybersecurity



National Preparedness Report

- States continue to have low overall awareness of risks to their information systems and low confidence in their ability to protect them against cyber threats. State Chief Information Security Officers (CISOs) view a lack of funding and skilled staff as top barriers to improving cybersecurity capabilities.

- In the 2012 SPR results, 78 percent of states and territories confirmed Cybersecurity as a high-priority capability, but only 15 percent rated cybersecurity training highly, the lowest across all capabilities.



National Preparedness Report

March 30, 2013

Homeland Security

The Survey

The Survey

- Understand the scope of the SLTT cyber security workforce
- Establish a baseline of current cyber security capabilities and proficiencies among the SLTT workforce
- Identify the general training needs of the cyber security workforce
- Enhance the cyber security proficiencies in the SLTT workforce

The Survey

- The MS-ISAC partnered with the Department of Homeland Security and the Department of State to collect data that would help identify the composition and capabilities of the SLTT cyber security workforce.
- The survey was distributed to each MS-ISAC member and each cyber-function employee was asked to respond to the survey.
- A total of 201 participants from 44 States and DC completed the survey.

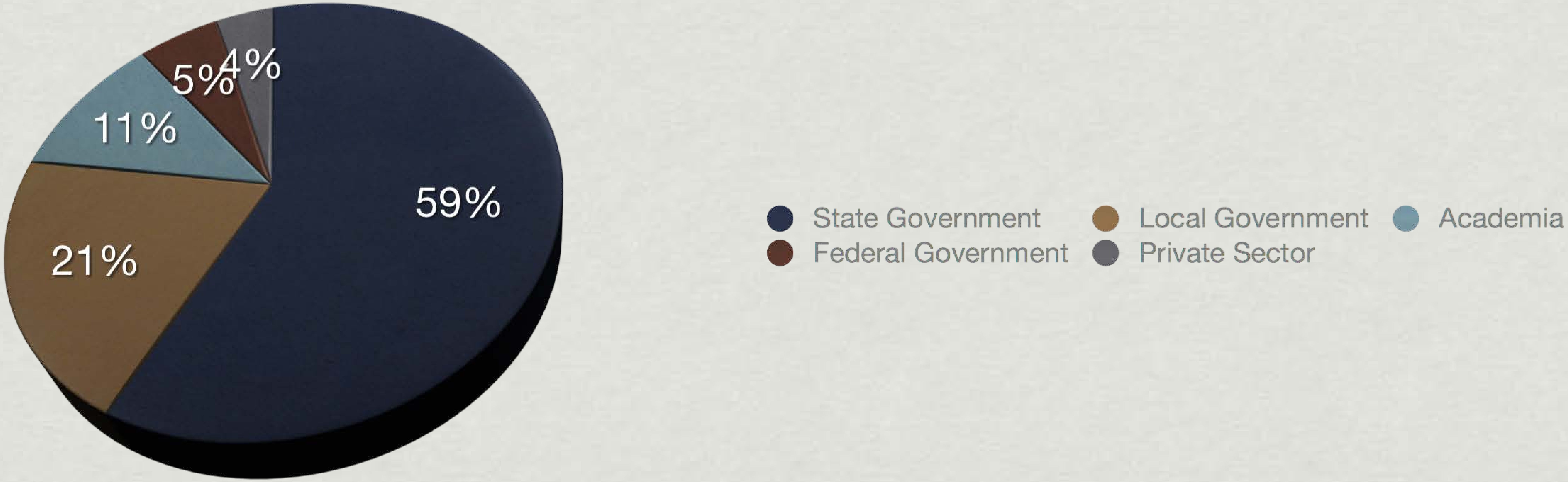
Survey Sections

Section	Description
Identification	Collects participant’s general (only required) information – such as name, email address (optional), length of time in field (required)
Environment	Captures the current state of cyber security workforce in their entity – including how many of cyber security professionals require additional technical training to adequately support the management and security of the entity’s IT infrastructure
Certifications	Captures the certifications required by the entity for the respondent to possess, and certifications acquired by participants relevant to cyber security
Proficiency Ratings	Captures participants’ average proficiency rating in each of the Speciality Areas
Training Needs	Indicates Specialty Areas in which participants felt more training would be beneficial to them in their current role

The survey was largely designed on the Specialty Areas identified in the framework developed by NICE.

Survey Results and Key Findings

Overview of Participants

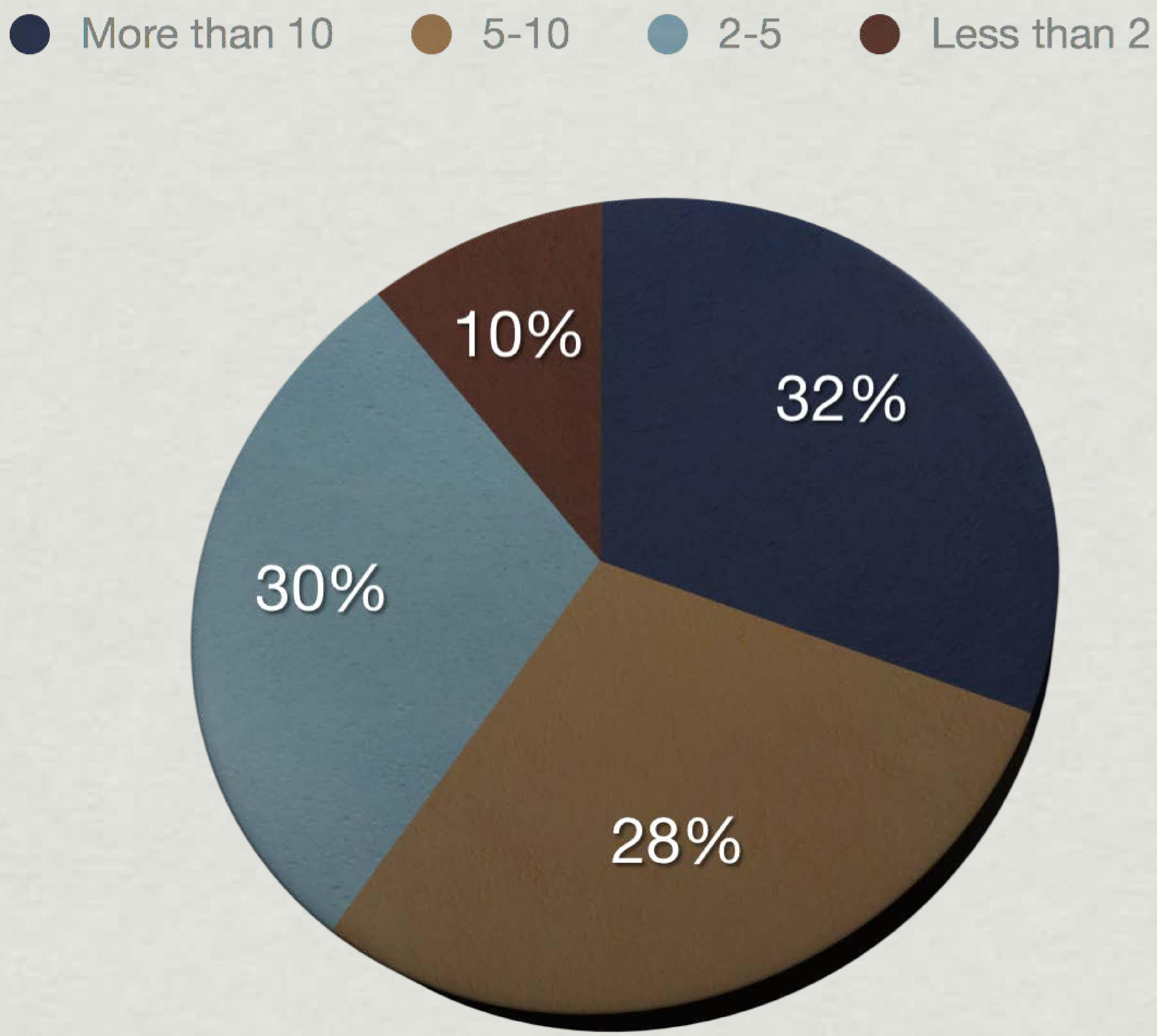


In addition, the most common role was Security Analyst (16%) followed by Information Systems Manager (14%) and CISO/Director of Security (11%).

Number of Years in the Field

- Participants had the opportunity to indicate the number of years of cyber security experience they possess.

- 68% of the participant population indicated they have less than 10 years of experience in the cyber security field.



Required Certifications

- The survey provided participants an opportunity to identify any certifications that are required for their position.
- Since the certification item in the survey was optional, the overall number of certifications required may not be a true representation.

Certification Required	# of Respondents
Certified Information Systems Security Professional	36
CompTIA Security+	22
Certified Information Security Manager	15
Certified Information Systems Auditor	13

Acquired Certifications

- The survey provided participants an opportunity to identify any certifications that are required for their position.
- Since the certification item in the survey was optional, the overall number of certifications acquired may not be a true representation of all the certification-holding participants.

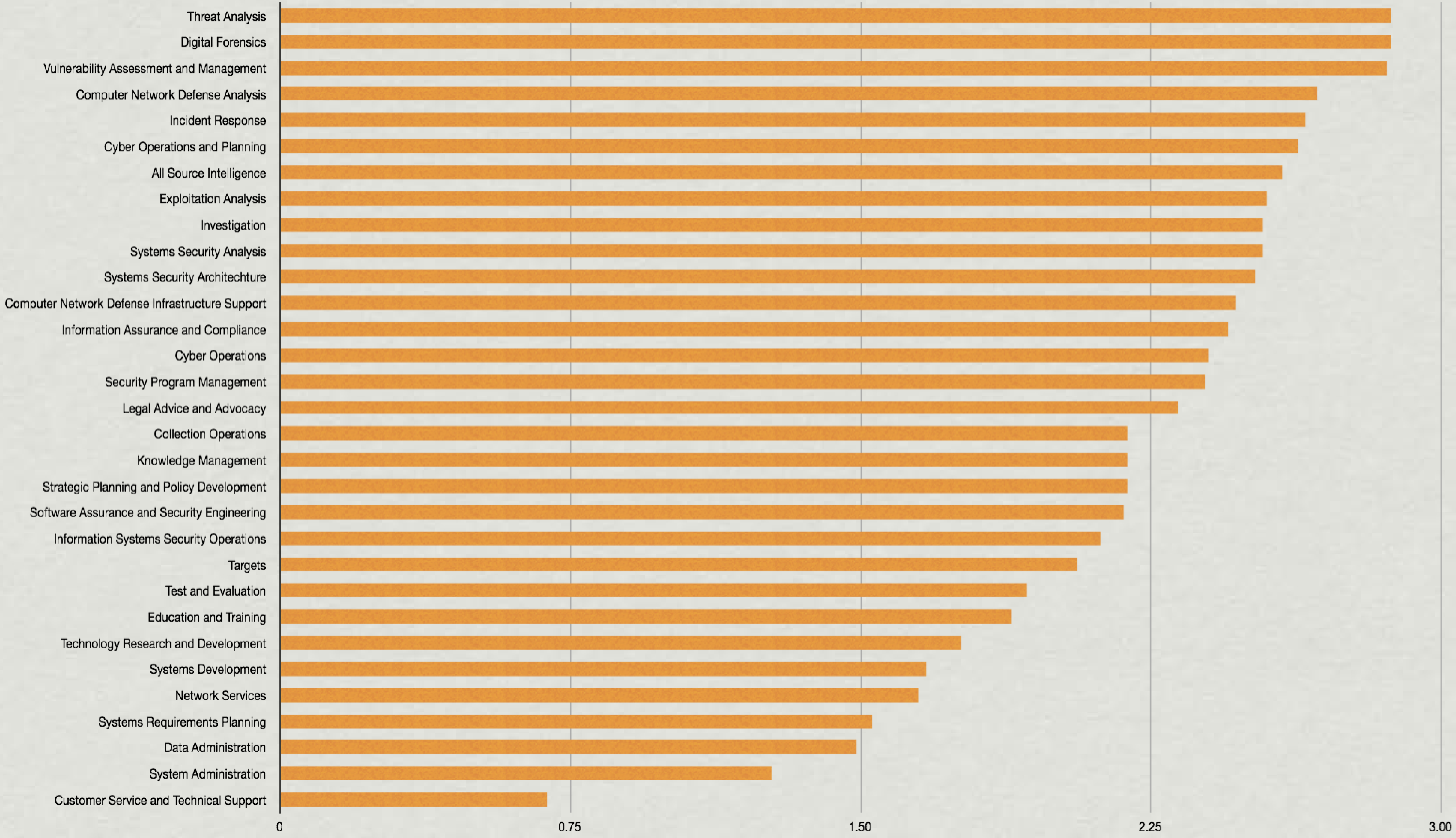
Certification Acquired	# of Respondents
Certified Information Systems Security Professional	33
CompTIA Security+	30
CompTIA Network+	15
Other/Not Listed	21

Proficiency Ratings

Survey participants self-assessed their current proficiency level in each of the Specialty Areas. In addition, participants indicated the optimal level of proficiency someone should demonstrate in their role.

- The highest average proficiency rating was in the **Customer Service and Technical Support**, followed by **System Administration**.
- The smallest identified gap was in **Customer Service and Technical Support**, in which 58% meets or exceeds optimal proficiency, followed by **Data Administration**.
- The largest identified gap was **Threat Analysis**, in which only 21% met or exceeded optimal proficiency.
- Other gaps identified: **Digital Forensics**, **Vulnerability Assessments**, **Computer Network Defense Analysis**, **Incident Response**.

Proficiency Ratings

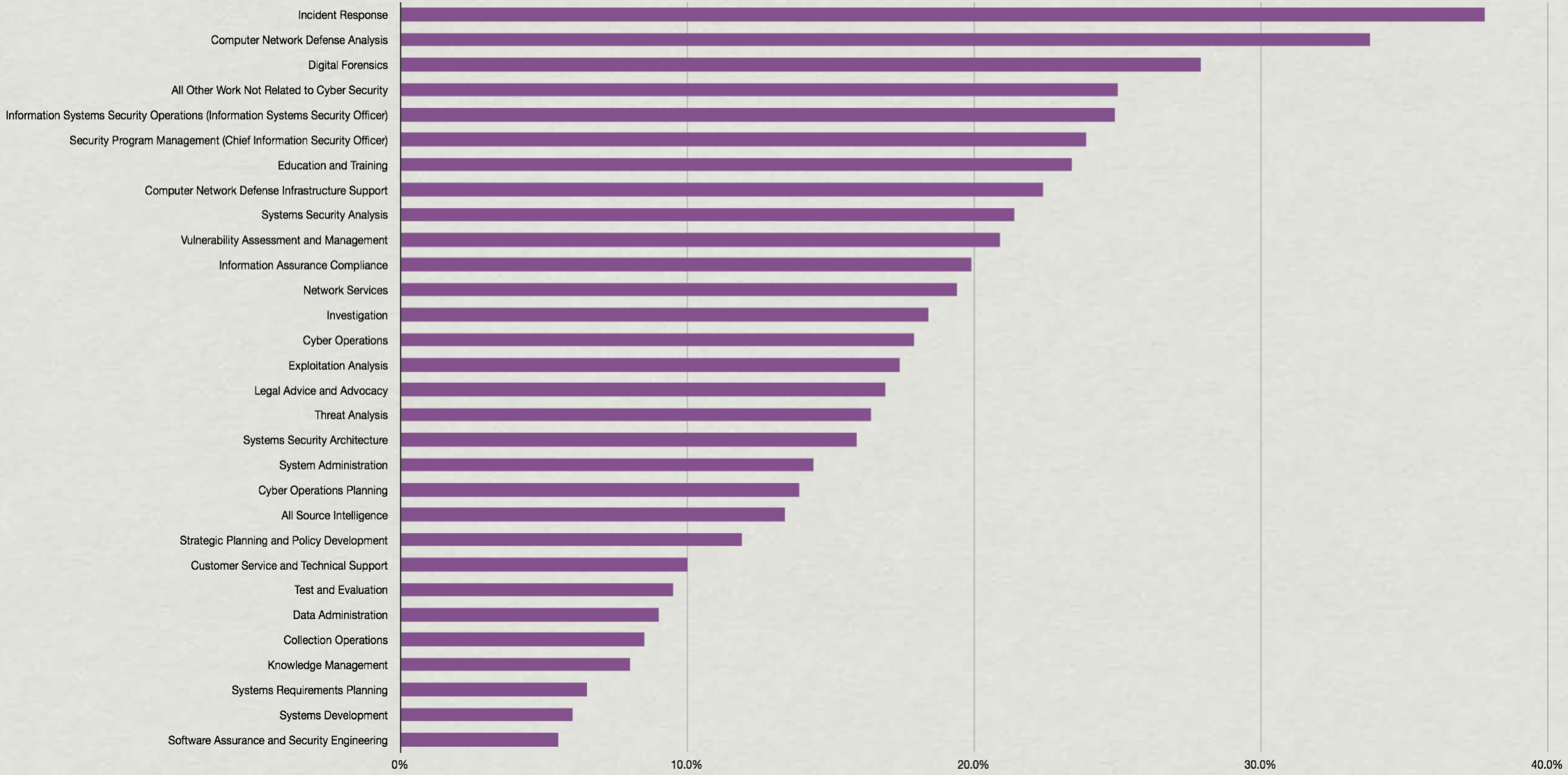


Training Needs and Gaps

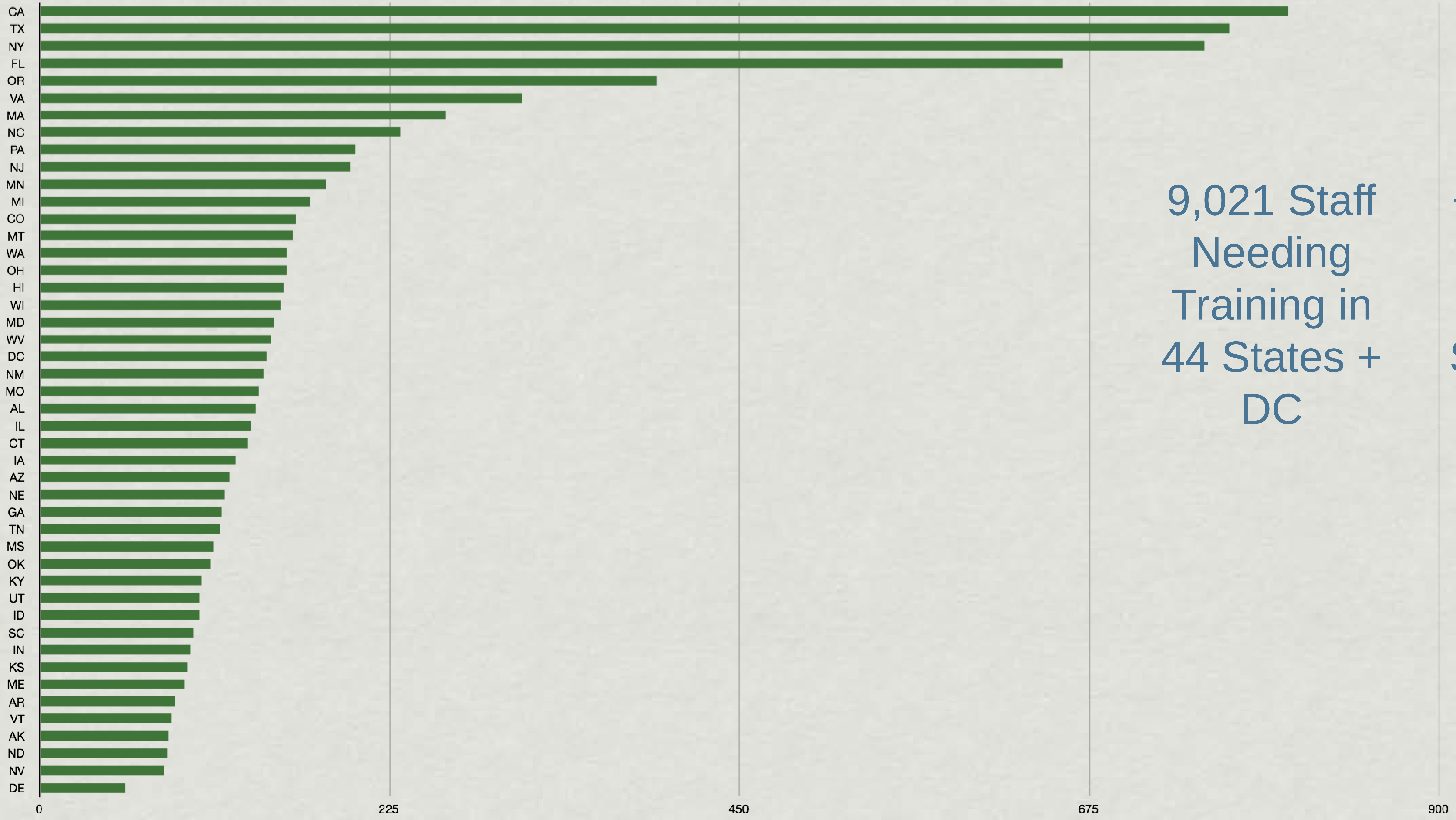
The Survey participants ranked the Specialty Areas that they believe additional training could benefit them in their current role.

- 75% of the assessment population prioritized one of the Specialty Area where training would make them more effective.
- 37.8% of the assessment population prioritized a training need in **Incident Response**.
- Participants also indicated strong need for training in **Computer Network Defense Analysis**, **Digital Forensics**, **Information Systems Security Operations** (Information Systems Security Officer), **Security Program Management**.
- As expected, the need is for more technical training.
- It could be assumed that a low proficiency level for a Specialty Area would indicate a higher need for training; however, in the case of the survey data, this is not true.

Training Needs and Gaps



Number of Staff Needing Additional Training



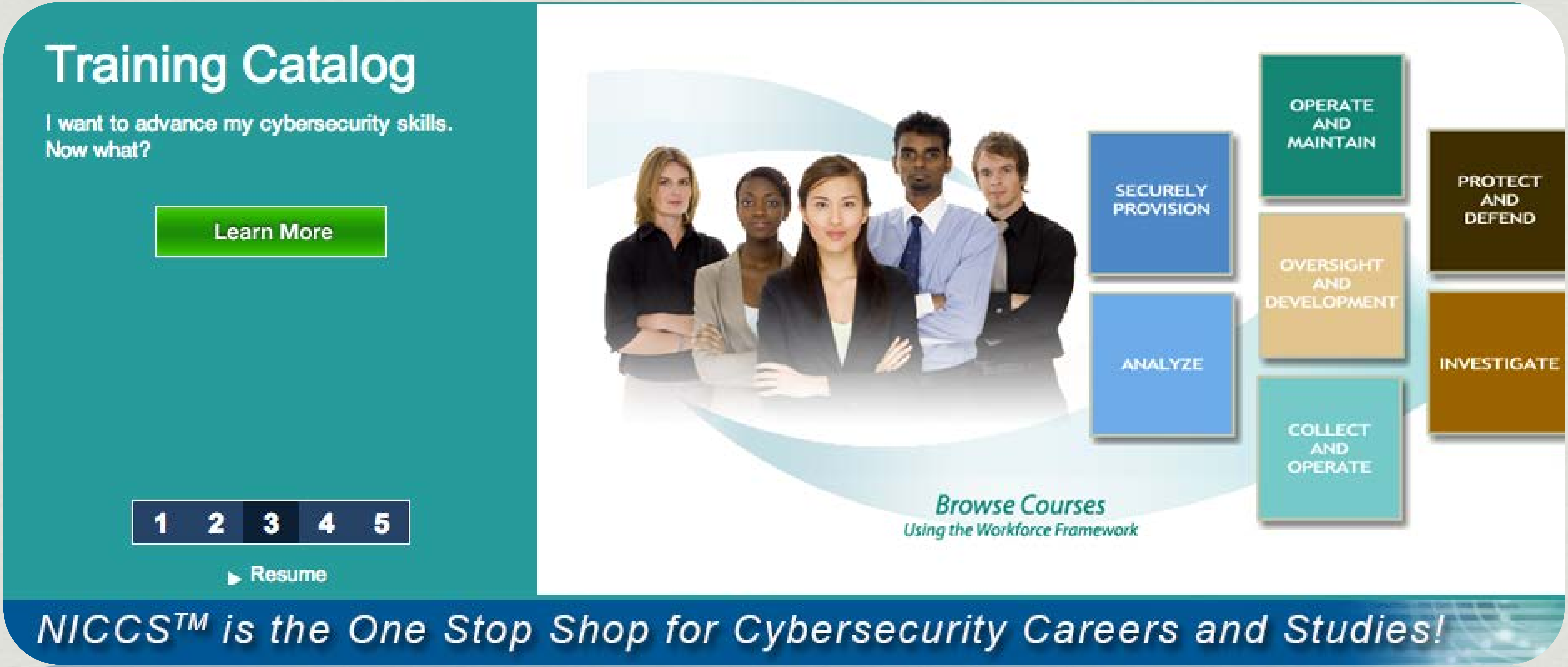
9,021 Staff Needing Training in 44 States + DC

~ 11,226 Staff Needing Training in 50 States + DC + 5 Territories

Fixing the Problem

Fixing the Problem

- Promote a national awareness program to empower all users to secure their parts of cyberspace
- Ensure adequate training and education programs exist to support the nation’s cyber security needs
- Increase the efficiency and availability of existing Federal cyber security training programs to the SLTT sector



Training Catalog

I want to advance my cybersecurity skills. Now what?

NICCS^{TM} is the One Stop Shop for Cybersecurity Careers and Studies!

As technology becomes increasingly more sophisticated, the demand for an experienced and qualified workforce to protect our nation's networks and information systems has never been higher. The National Institute for Cybersecurity Careers & Studies (NICCS) serves as a national resource for cybersecurity awareness, education, training, and career opportunities. NICCS is the implementation of the National Initiative for Cybersecurity Education (NICE), whose goal is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. NICE is a nationally-coordinated effort that focuses on cybersecurity awareness, education, workforce structure, and training/professional development. NICCS takes the information developed by NICE and makes it available to the public. Visit www.niccs.us-cert.gov to learn more.

Center for Internet Security®

Asif Ismail

Program Manager

asif.ismail@cisecurity.org

(518) 880-0686