Deciphering the National Cybersecurity Strategy:
Implications for Cybersecurity Professionals

Niloufer Tamboly, CISSP, CPA

Disclaimer

The views expressed in this presentation and during the session are my personal opinions and do not reflect the official policy or position of my employers.

Niloufer Tamboly

👩🏽‍💻 Work

Verizon – Risk Management

🧑🏽‍🏫 Lecturer

Rutgers University – 401 level class

🎓 Education MBA in Security Assurance

🔖 Certifications CISSP, CPA, CISA, CFE, CIA, CGMA, CDPSE, Open FAIR

🔔 Patents

Establishing An Alternate Call Path Using Short-Range Wireless Technology
System For And Method of Generating Visual Passwords

🤝 Volunteer

Cofounder - Step Up Skill and (ISC)2 New Jersey Chapter
Organizer - CISSP & CCSP Exam Study Group

National Cybersecurity Strategy

Defend critical infrastructure

1.1: Establish Cybersecurity Requirements to support National Security and Public Safety

1.2: Scale Public-Private Collaboration

1.3: Integrate Federal Cybersecurity Centers

1.4: Update Federal Incident Response Plans and Processes

1.5: Modernize Federal Defenses

Disrupt and dismantle threat actors

2.1: Integrate Federal Disruption Activities
2.2: Enhance Public-Private Operational Collaboration to Disrupt Adversaries
2.3: Increase the Speed and Scale of Intelligence Sharing and Victim Notification
2.4: Prevent Abuse of U.S.-Based Infrastructure
2.5: Counter Cybercrime, Defeat Ransomware

Shape market forces to drive security and resilience

3.1: Hold the Stewards of our data accountable
3.2: Drive the Development of Secure IoT Devices
3.3: Shift Liability for Insecure Software Products and Services
3.4: Use Federal Grants and Other Incentives to Build in Security
3.5: Leverage Federal Procurement to Improve Accountability
3.6: Explore a Federal Cyber Insurance Backstop

Invest in a resilient future

4.1: Secure the Technical Foundation of the Internet
4.2: Reinvigorate Federal Research and Development for Cybersecurity
4.3: Prepare for our Post-Quantum Future
4.4: Secure our Clean Energy Future
4.5: Support Development of a Digital Identity Ecosystem
4.6: Develop a National Strategy to Strengthen our Cyber Workforce

Forge international partnerships to pursue shared goals

5.1: Build Coalitions to Counter Threats to our Digital Ecosystem

5.2: Strengthen International Partner Capacity

5.3: Expand U.S. Ability to assist Allies and Partners

5.4: Build Coalitions to Reinforce Global Norms of Responsible State Behavior

5.5: Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services

So what? and why should I care?

Overemphasis on federal involvement

Lack of clarity

Insufficient funding

Conflicting priorities

Workforce challenges

International cooperation

Impact

Increased Responsibility

Cybersecurity professionals have a heightened responsibility to contribute to the strategy's objectives, such as protecting government networks and data.

Advanced Skills

There is a growing demand for advanced technical skills, as cyber threats become more sophisticated and prevalent.

Cross-Sector Collaboration

Cybersecurity professionals are expected to collaborate within their organizations and sectors to share threat intelligence and best practices.

Ethical Standards

Maintaining strong ethical standards and integrity is crucial, as the strategy emphasizes the importance of trust in cyberspace.

Policy Understanding

Professionals need a deep understanding of the evolving cybersecurity policy landscape to align their efforts with national objectives.

International Cooperation

The strategy's focus on international cooperation means professionals may engage with counterparts in other countries and adhere to international cybersecurity norms.

Innovation

Cybersecurity professionals must continuously innovate and adapt to evolving threats, technologies, and strategies.

Government Contracts

An increased emphasis on government network protection means more opportunities for cybersecurity professionals in government contracting roles.

Training and Education

The strategy highlights the need for ongoing training and education to keep up with evolving threats and best practices.

Career Resilience

Staying informed about the strategy and its changes is crucial for career resilience in a fast-paced, ever-changing cybersecurity landscape.

Let’s connect in