Homeland Security: Information Assurance Challenges and Opportunities

Building the National Cyber Security Division

The Homeland Security Act and national strategies direct DHS to take the lead on cyber security

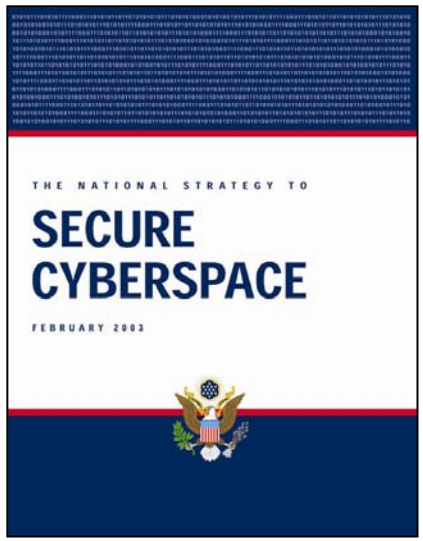
One Hundred Seventh Congress
of the
United States of America

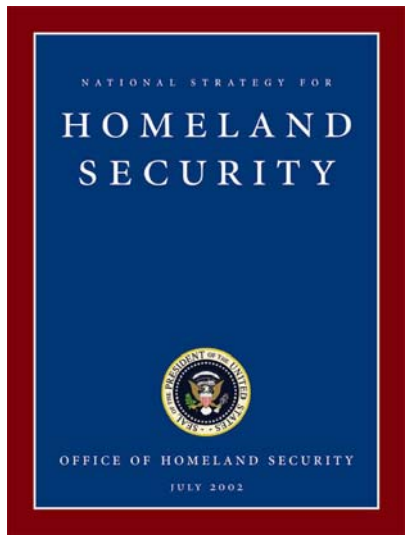
AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the twenty-third day of January, two thousand and two

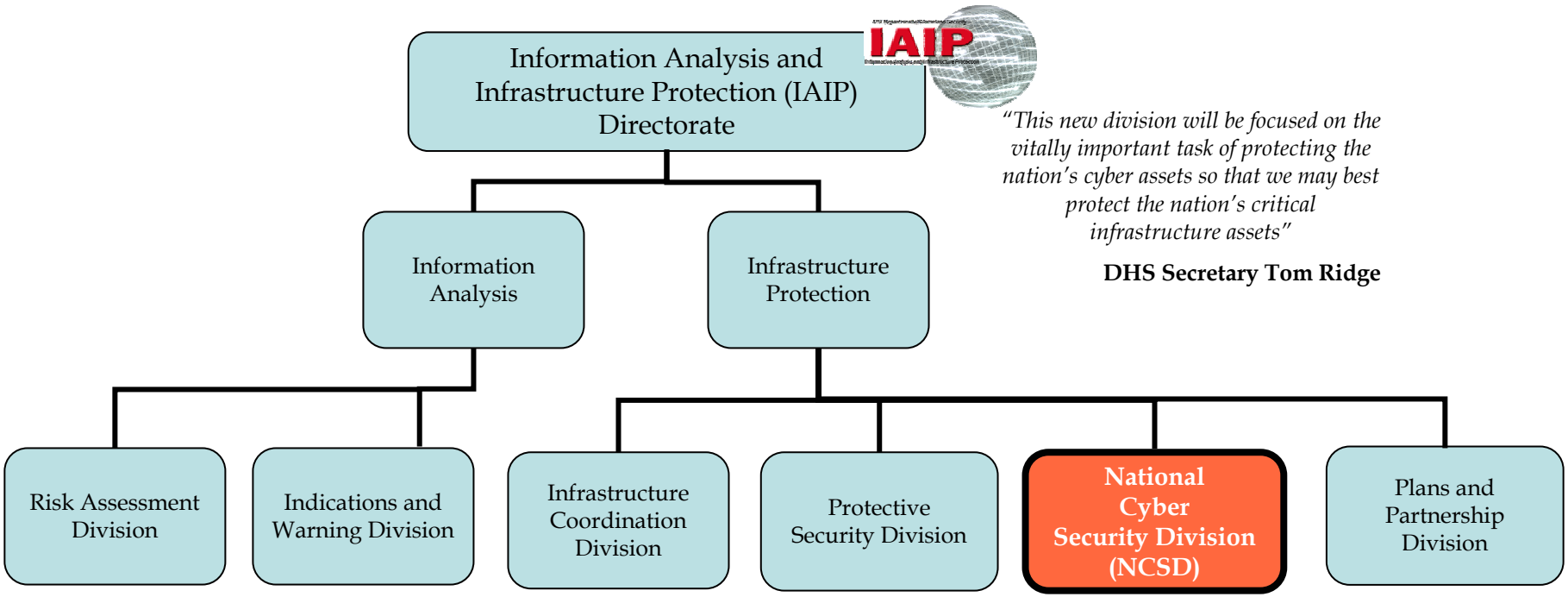
An Act

To establish the Department of Homeland Security, and for other purposes.





As a result, DHS established the National Cyber Security Division (NCSD) as the dedicated Federal focal point for cyber security



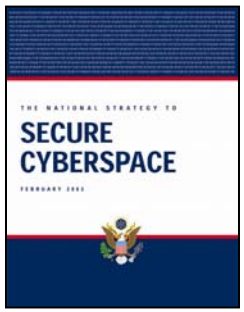
"This new division will be focused on the vitally important task of protecting the nation's cyber assets so that we may best protect the nation's critical infrastructure assets"

DHS Secretary Tom Ridge

Current NCSD operations are organized into three functional areas:

- Key NCSD Functional Areas
  - Risk, Threat, Vulnerability Identification & Reduction
  - U.S. Computer Emergency Response Team (US-CERT)
  - Outreach, Awareness, & Training

These three key mission areas are in alignment with the National Strategy to Secure Cyberspace



National Strategy to Secure Cyberspace

	Three Key Mission Areas of NCSD		
	Risk, Threat, & Vulnerability Reduction	U.S. Computer Emergency Response Team (US-CERT)	Outreach, Awareness, & Training
Strategic Objectives of the National Strategy to Secure Cyberspace			
Prevent cyber attacks against America's Critical Infrastructure	✓	✓	✓
Reduce National vulnerability to cyber attacks	✓	✓	✓
Minimize damage and recovery time from cyber attacks that do occur	✓	✓	✓
Critical Priorities of the National Strategy to Secure Cyberspace			
A National Cyberspace security response system		✓	
A National Cyberspace security threat & vulnerability reduction program	✓		
A National Cyberspace security awareness training program			✓
Securing Governments' cyberspace	✓	✓	✓
National Security & International Cyberspace Security Cooperation	✓	✓	✓

The NCSD is leveraging relationships with and capabilities of public and private sector partners to support current operations

Partnerships	Functional Area Description
• Organizations with functions that are now resident in NCSD – NIPC – FedCIRC – NCS – CIAO • Government entity partners – Law enforcement – Federal, State and Local government organizations – NASCIO/Multi State ISAC – HSC • Private sector partners – Key industry associations and groups – ISAC's	• Risk, Threat, Vulnerability Identification & Reduction – Leverage, design, and lead implementation of methodologies and best practices with our partners to assess risks and threats, and to reduce vulnerabilities to attacks • U.S. Computer Emergency Response Team (US-CERT) – Implement US-CERT by consolidating government organizations and leveraging our National and international leadership and expertise across the public sector, the private sector, and academia • Outreach, Awareness & Training – Design and lead implementation of training and awareness efforts and campaigns that use a multi-level approach to education industry, government, and the public on the importance of their roles in National cyber security

Activities

- Appointed Director of the National Cyber Security Division
- DHS announced creation of U.S. Computer Emergency Response Team (US-CERT)
- Coordinating Cyber Situational Awareness Project
- Planning Cyber Summit

Activities *cont.*

- Standardizing response capabilities
- Developing Best Practices to assist in vulnerability reduction
- Reaching out to home users and small businesses
- Promoting Private Sector Certifications Programs
- Increasing effectiveness of Federal Training Programs

The Ultimate Goal….

A Culture of Cyber Security

Contact Information

Sallie McDonald
Department of Homeland Security
Information Analysis & Infrastructure Protection

Phone: (202) 708-7000
www.dhs.gov