# DHS,
# National Cyber Security Division Overview

Hun Kim, Deputy Director

Strategic Initiatives

Information Analysis and Infrastructure
Protection Directorate

www.us-cert.gov

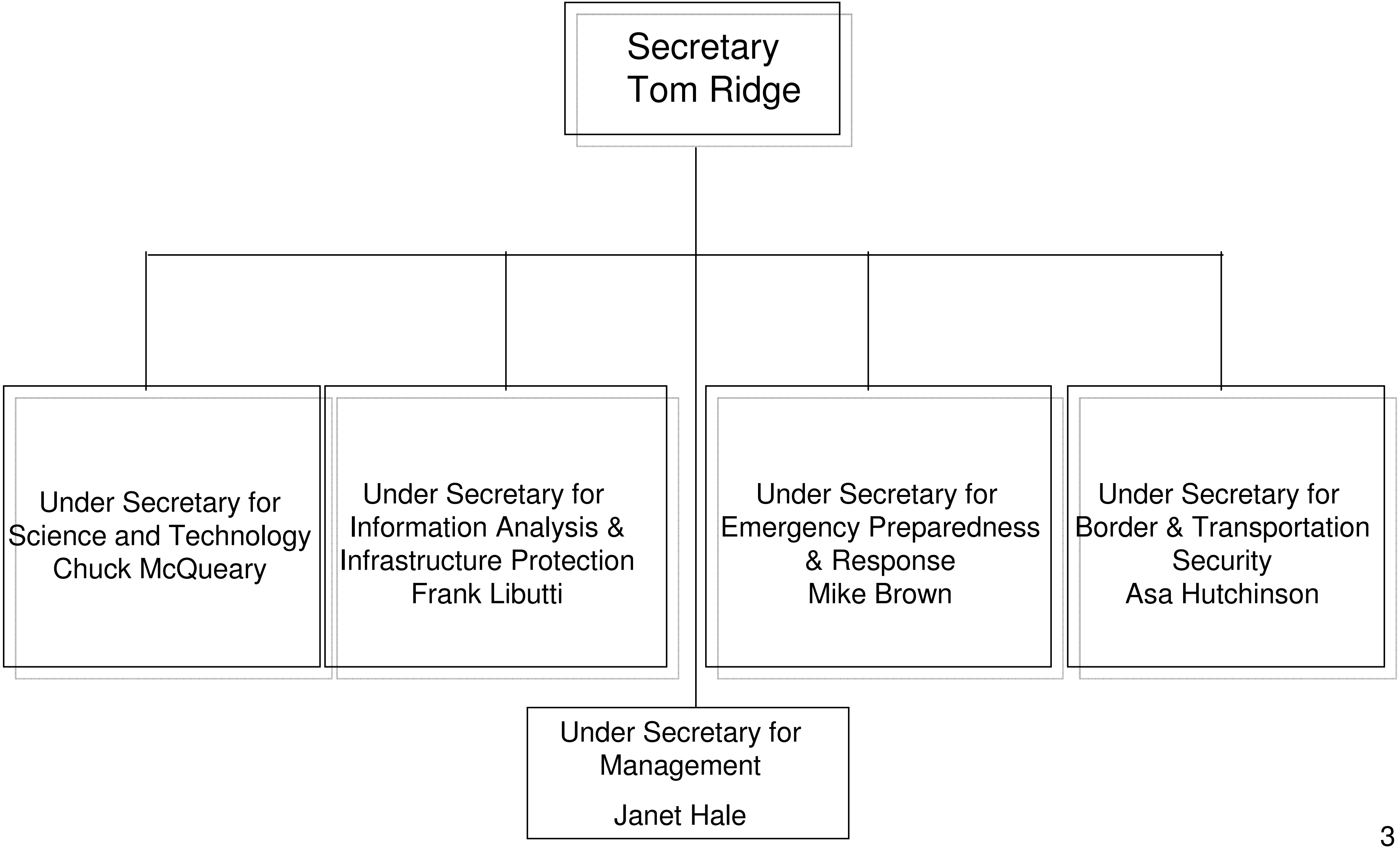
# The strategy of DHS, as defined by the Nation Strategy for Homeland Security, consists of three key objectives

US-CERT

## Three Key Objectives of the National Strategy for Homeland Security

| Key Objective I | Key Objective II | Key Objective III |
|---|---|---|
| Prevent terrorist attacks within the United States | Reduce America's vulnerability to terrorism | Minimize the damage and recover from attacks that do occur |

# Department of Homeland Security



Secretary
Tom Ridge

Under Secretary for
Science and Technology
Chuck McQueary

Under Secretary for
Information Analysis &
Infrastructure Protection
Frank Libutti

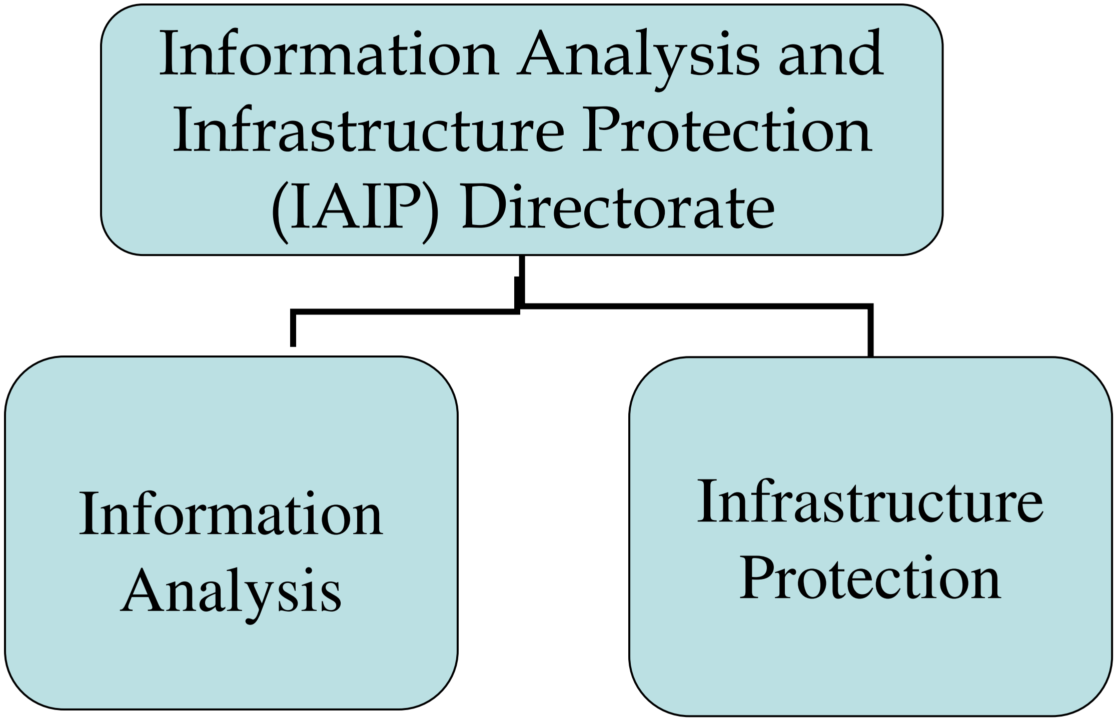
Under Secretary for
Emergency Preparedness
& Response
Mike Brown

Under Secretary for
Border & Transportation
Security
Asa Hutchinson

Under Secretary for
Management

Janet Hale

# IAIP Directorate

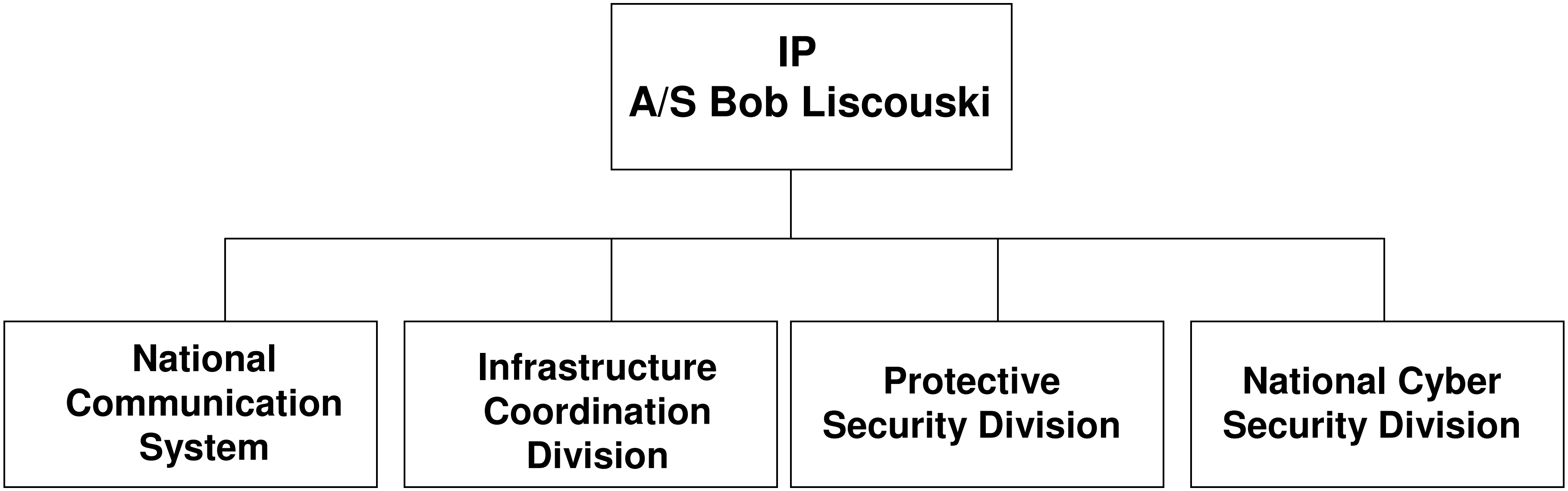


Information Analysis and Infrastructure Protection (IAIP) Directorate

Information Analysis

Infrastructure Protection

# The structure of Infrastructure Protection Directorate



IP
A/S Bob Liscouski

National Communication System

Infrastructure Coordination Division

Protective Security Division

National Cyber Security Division

IP, in partnership with IA and federal, state, local, private, and international entities protects America’s critical infrastructures.

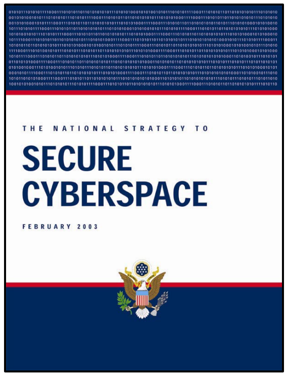
# NCSD Mission

**Serve as the national focal point for cyber security and implement the National Strategy to Secure Cyberspace**

Mission components include:

National Cyberspace Security Response System
National Cyber Security Threat and Vulnerability Reduction Program
National Cyberspace Security Awareness and Training Program
Securing Governments’ Cyberspace
International Cyberspace Security Cooperation

…to implement the National Strategy…



THE NATIONAL STRATEGY TO
SECURE
CYBERSPACE
FEBRUARY 2003

# NCSD Overview

| | |
|---|---|
| US-CERT | •U.S. Computer Emergency Readiness Team |
| Strategic Initiatives | •Cyber Security improvement initiatives |
| Cyber Coordination | •Outreach, awareness, coordination |

# US-CERT

| | |
|---|---|
| The National Readiness and Response System | • Rapid identification, information exchanges, and remediation can mitigate damage.<br>• Response system will involve public and private institutions and cyber centers to perform analyses, conduct watch and warning, enable information exchange, and facilitate restoration efforts. |
| Securing Government's Cyberspace | • Federal, State, and Local Governments' systems protection and resilience.<br>• Continuously assess threats and vulnerabilities to cyber systems. |
| Cyber Interagency Incident Management Group | • Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. |
| 24 x 7 Operations Center | • A focal point for cyberspace security. Facilitate watch interactions between and among agencies, governments, private sector, academia, and international organizations. |
| National Cyber Alert System | • Identify, analyze, and prioritize emerging vulnerabilities and threat. Provide credible and timely information on cyber security issues. Provide actionable information to empower all citizens to secure their portion of cyberspace. |

# NCSD Strategic Initiatives

US-CERT

| | |
|---|---|
| CIP – Cyber Security | • HSPD 7 Cyber CIP Plan for Vulnerability Assessment and Reduction |
| Software Assurance | • Evaluate software development processes, procedures, & testing tools to mitigate risks and assure software integrity |
| Training & Education | • Develops programs with training and education institutions to increase adequately trained IT security personnel |
| R&D, Standards, & Best Practices | • Identifies R&D requirements and cyber security standards issues, and assembles and distributes best practices |
| Control Systems | • Maintain a nationwide control systems cyber security situational awareness and provide incident response capability |
| Exercise Planning & Coordination | • Plans and coordinates cyber security exercises with internal and external DHS stakeholders |

# NCSD Cyber Coordination

US-CERT

| | |
|---|---|
| Outreach and Awareness | • promote cyber security awareness among the general public and within key communities |
| Federal-State Coordination | • Maintains relationships with governmental cyber security professionals to coordinate and share information about cyber security initiatives. |
| Law Enforcement / Intelligence Coordination | • Coordinate between law enforcement, national security, and defense agencies to ensure that criminal matters are well coordinated among those agencies. |
| Partnership | • Develops partnership program to promote public-private coordination and collaboration on cyber security issues. |
| External Communications | • Maintains website and other communications channels to provide information about NCSD, US-CERT, and related events & information to the general public. |

# DHS, S&T Directorate - Cyber Security Research & Development

US-CERT

Science and Technology Directorate (S&T)

- Serves as the primary research and development arm of the Department, utilizing our nation's scientific and technological resources to provide federal, state, and local officials with the technologies and capabilities necessary to protect the homeland.
  - Advises Secretary regarding R&D efforts and priorities
  - Establishes, conducts, and coordinates basic and applied research, development, testing, and evaluation (RDT&E) activities
  - Establishes priorities for and directs, funds, and conducts RDT&E, and procures technology and systems

# Road Ahead

US-CERT

- Critical Infrastructure Protection
  - Integration of Physical Security and Cyber Security
  - Control Systems
- Software Assurance
- National Cyber Exercise
- International Cooperation

Hun Kim

Hun.Kim@dhs.gov

(202) 401-4269