

Command, Control and Interoperability Division

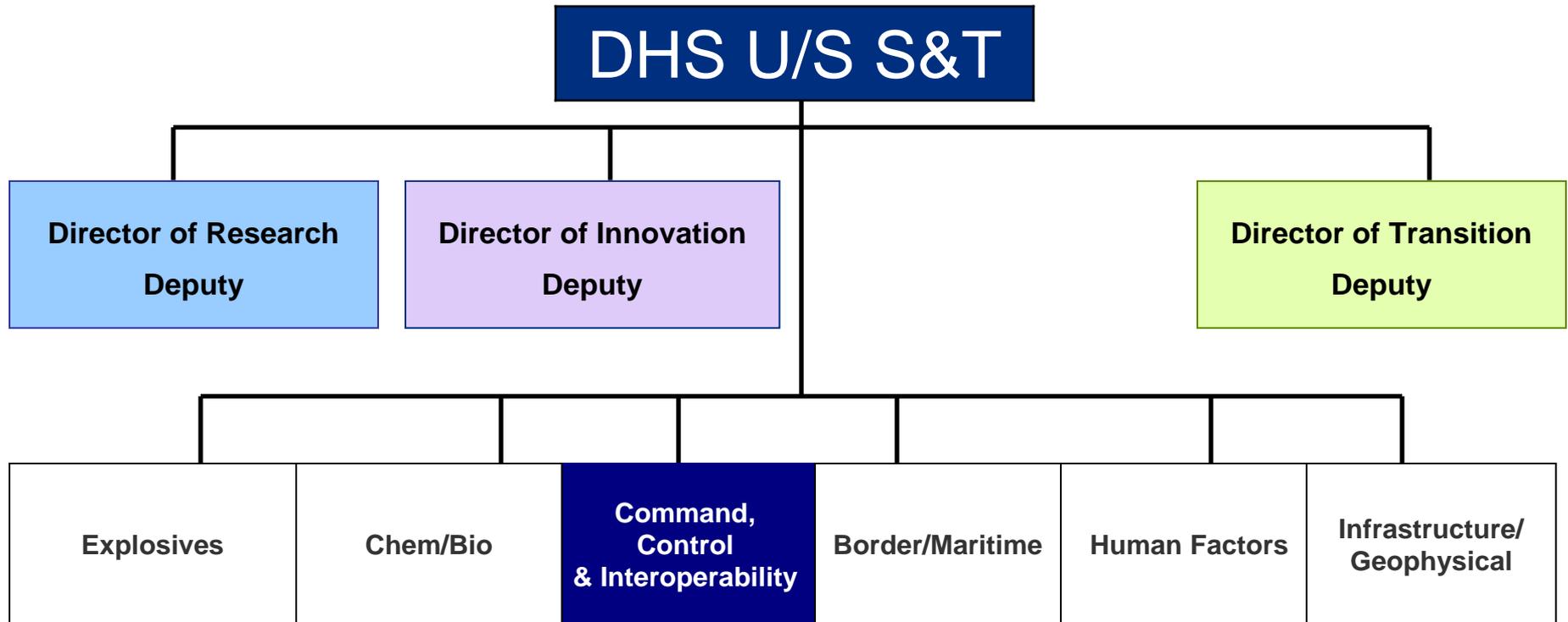
Dr. David Boyd
Director
Command, Control and Interoperability
Science and Technology Directorate
U.S. Department of Homeland Security
March 3, 2009

Science and Technology Directorate Goals



- Accelerate delivery of enhanced technological capabilities to meet requirements and fill capability gaps
- Establish a GS-manned, world-class S&T management team to deliver the technological advantage necessary to ensure DHS Agency mission success and prevent technology surprise
- Provide leadership, research and educational opportunities and resources to develop the necessary intellectual basis to enable a national S&T workforce to secure the homeland

DHS S&T Directorate: Organization



Command, Control and Interoperability

Mission

Through a practitioner-driven approach, the Command, Control and Interoperability (CCI) Division creates and deploys information resources to enable seamless and secure interactions among homeland security stakeholders.

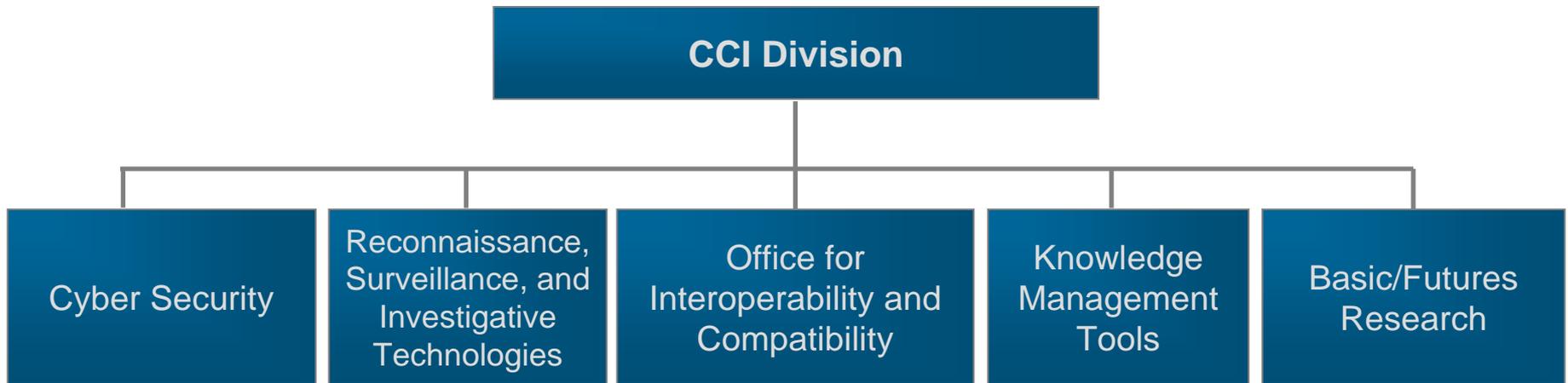


Vision

Stakeholders have comprehensive, real-time, and relevant information to create and maintain a secure and safe Nation.

CCI Division Organization

Managed by the S&T Directorate, CCI delivers on its mission through five program areas.



Command, Control and Interoperability

Information

Identify

Manage

Communicate

Analyze

Visualize

Protect

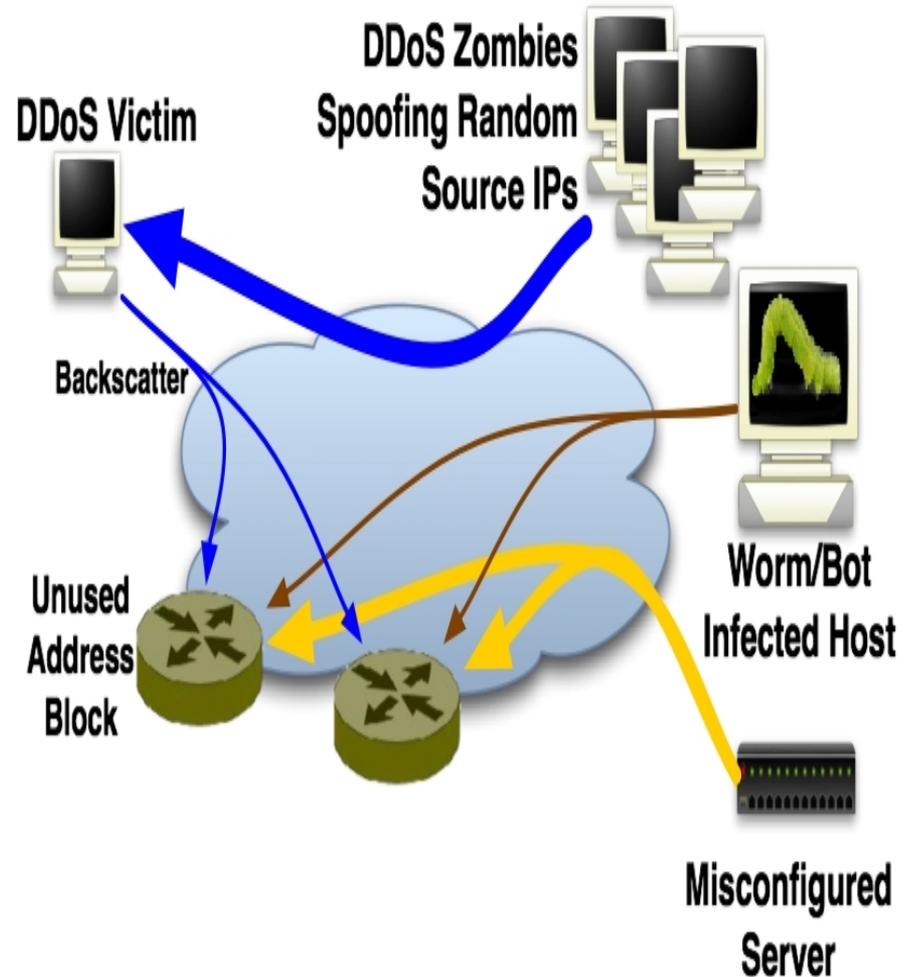


Cyber Security

- Secures critical infrastructure and coordinates efforts to improve the existing cyber infrastructure
- Focuses on priorities established in the President's *National Strategy to Secure Cyberspace* and needs identified by critical infrastructure external stakeholders
- Addresses cyber security requirements in support of DHS operational missions in critical infrastructure protection

Program Areas

- Information Infrastructure Security
- Cyber Security Research Tools and Techniques
- Next Generation Technologies



Domain Name System Security Initiative

- Through its Domain Name System Security (DNSSEC) initiative, CCI is working to provide guaranteed authenticity and integrity for Internet communications and is ensuring that Internet users reach correct/valid Internet sites.



- DNSSEC consists of a hierarchy of cryptographic signatures that assures the integrity of DNS queries, protects against tampering, and strengthens infrastructure security—resulting in secure Internet operations.
- The CID Cyber Security program area aims for all DNS traffic on the Internet to be DNSSEC-compliant.



IronKey Technology

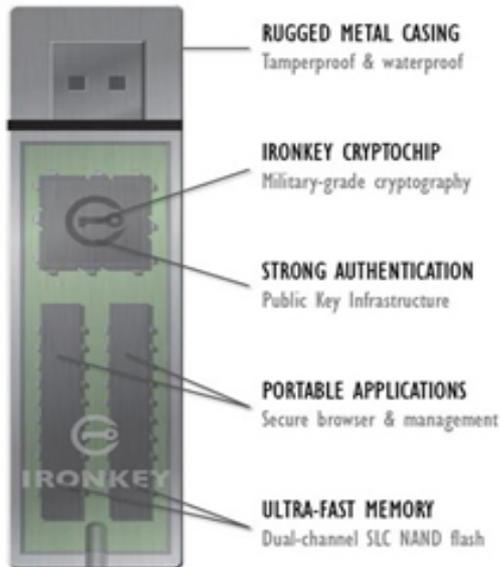
- provides secure web browsing, cryptographic authentication, end point security, self-service password recovery, and secure password management.
- user data is encrypted with advanced encryption standard (AES) hardware

Security First

No one can access files stored on an IronKey unless they authenticate their identity with the correct password. All encryption and password verification are performed in hardware and cannot be disabled by malware or a careless user.

Easy to Deploy and Maintain

The IronKey does not require any software or drivers to be installed and it works on Windows XP and Vista without administrator privileges. Once initialized, the IronKey Basic also works on Linux systems and on Macintosh OSX.



Reconnaissance, Surveillance, and Investigative Technologies

- Develop and evaluate individual sensor technologies, fusion of multiple sensors, and examination of new sensor technologies.
- Develop integrated technology platforms to collect, share, and disseminate information.
- Develop advanced investigative and crime scene forensic tools.
- Support the technical rationale for policies and privacy issues associated with these applications.
- Initiate R&D activities with intelligence and defense organizations.



Office for Interoperability and Compatibility

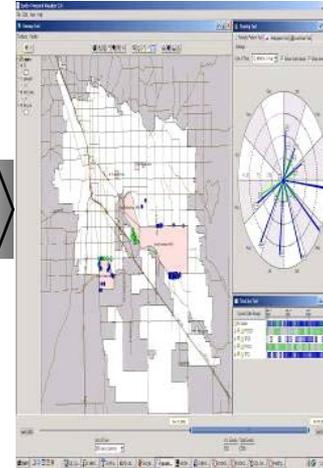
- works with emergency response community and Federal partners to improve local, tribal, state, and Federal emergency preparedness and response
- OIC programs address both data and voice interoperability



- supports the development of technologies and messaging standards that help emergency responders manage incidents and exchange information in real time.

Knowledge Management Tools

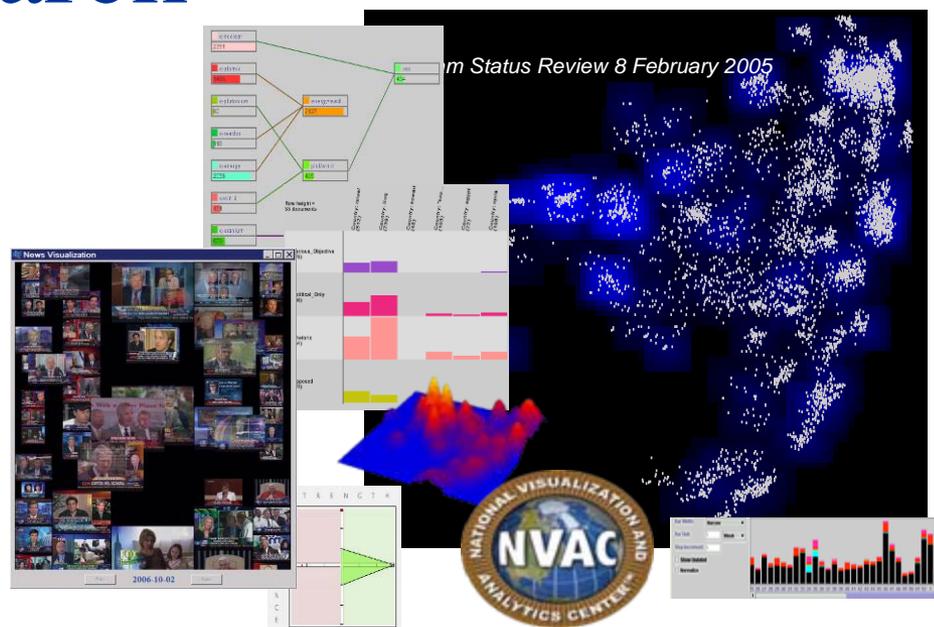
- Provides knowledge management capabilities to reduce the risk of terrorist attacks and to prepare for and respond to natural and man-made disasters.



- Develops tools and methods to process and analyze massive amounts of information that are widely dispersed and in multiple forms.
- Works collaboratively to complement efforts in the intelligence, law enforcement, and homeland security communities.

Basic/Futures Research

- Information and intelligence systems research
- Comprehensive, timely threat awareness
- Accurate consequence analysis
- Effective risk management approach to homeland security



- **Visual Analytics and Precision Information Environments Program:** Visually-based mathematical methods and computational algorithms for discovering, comprehending, and manipulating diverse data, and applying the resulting knowledge to anticipate terrorist incidents and/or catastrophic events.
- **Discrete-Element Computing, Privacy, and Forensics Program:** Software algorithms and hardware architectures for extracting and managing data, assessing threats and consequences, ensuring information privacy, securing the cyber infrastructure, and ensuring telecommunications interoperability.

Command, Control and Interoperability

Information

Identify

Manage

Communicate

Analyze

Visualize

Protect





Homeland Security