Cybersecurity T&E: Closing the Gap between Authorities to Operate and Operating Securely

24 February 2015

Dr. Steven J Hutchison
Director, Test and Evaluation
Acting Director, Capability Development Support

Homeland Security
Science and Technology

Homeland Security
Science and Technology

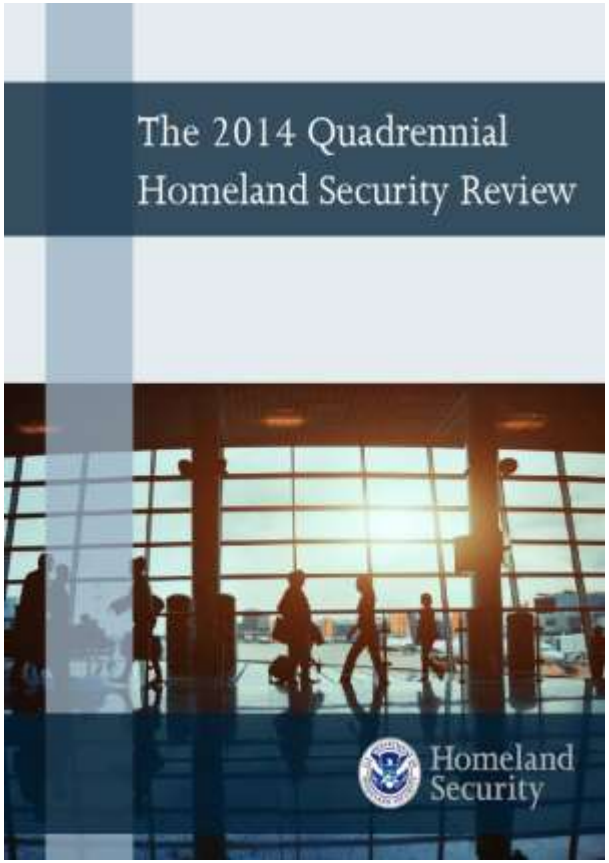
The Gap

Our adversaries are not limited to exploiting vulnerabilities within the set of security controls defined by the Risk Management Framework.

Robust Cybersecurity T&E can help Programs close the gap.

Homeland Security
Science and Technology

Department of Homeland Security



Mission

- Prevent Terrorism and Enhance Security
- Secure and Manage Our Borders
- Enforce and Administer Our Immigration Laws
- Safeguard and Secure Cyberspace
- Strengthen National Preparedness and Resilience

http://www.dhs.gov/quadrennial-homeland-security-review-qhsr

Homeland Security
Science and Technology

Safeguard and Secure Cyberspace

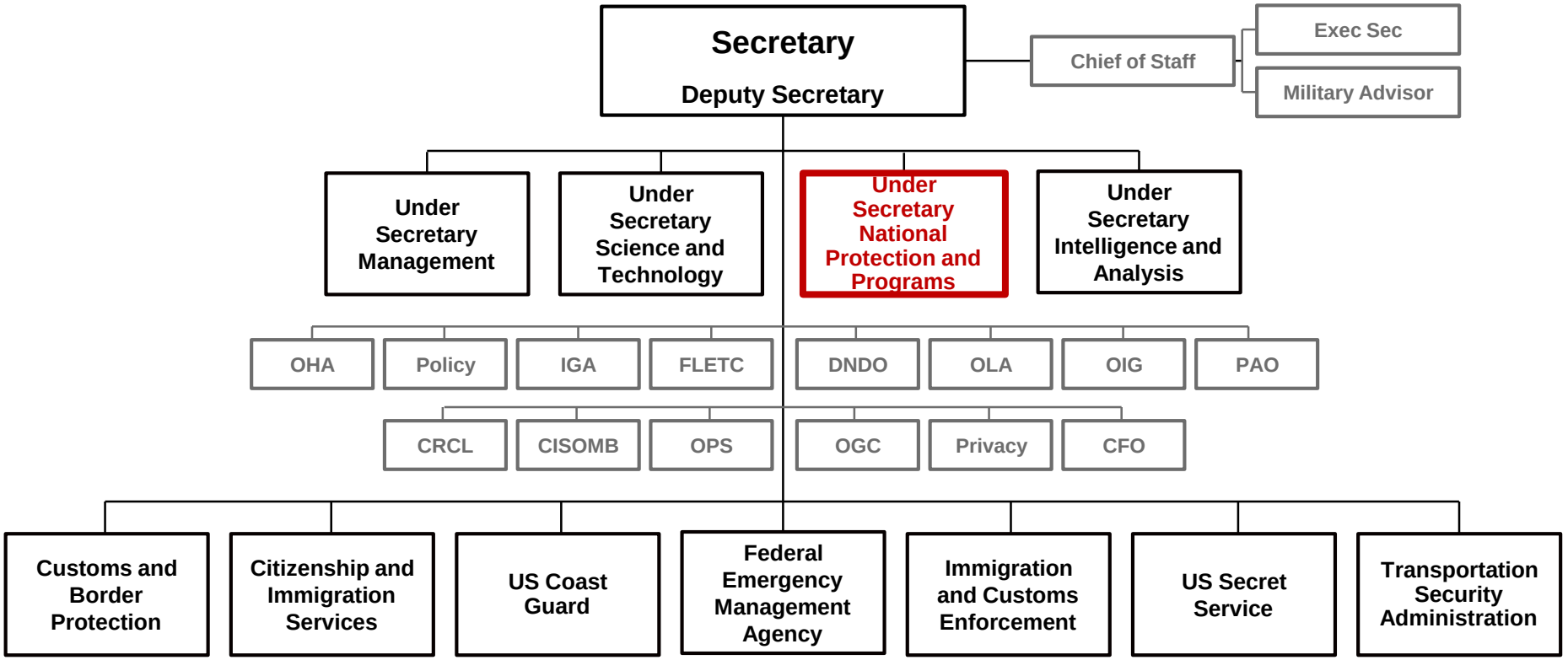
Areas of Emphasis

- Strengthen the Security and Resilience of Critical Infrastructure
- Secure the Federal Civilian Government Information Technology Enterprise
- Advance Law Enforcement, Incident Response, and Reporting Capabilities
- Strengthen the Ecosystem

http://www.dhs.gov/quadrennial-homeland-security-review-qhsr

Homeland Security
Science and Technology

Department of Homeland Security



Homeland Security
Science and Technology

National Cybersecurity and Communications Integration Center (NCCIC)

NPPD Mission

We lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

Homeland Security
Science and Technology

The DETER Project

cyber **DE**fense **T**echnology **E**xperimental **R**esearch

- A research program:
  - To advance capabilities for experimental cybersecurity research
- A testbed facility:
  - To serve as a publicly available national resource…
- A community building activity:
  - To foster and support collaborative science
- Funded by the Department of Homeland Security, National Science Foundation, and Department of Defense

http://deter-project.org/

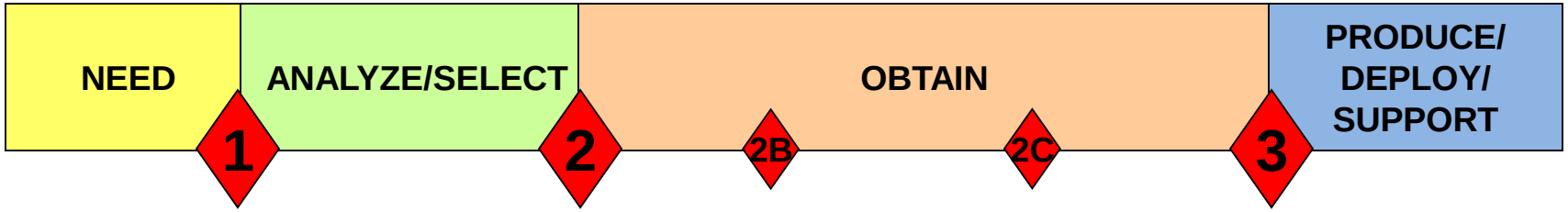
Homeland Security
Science and Technology

DETER Lab

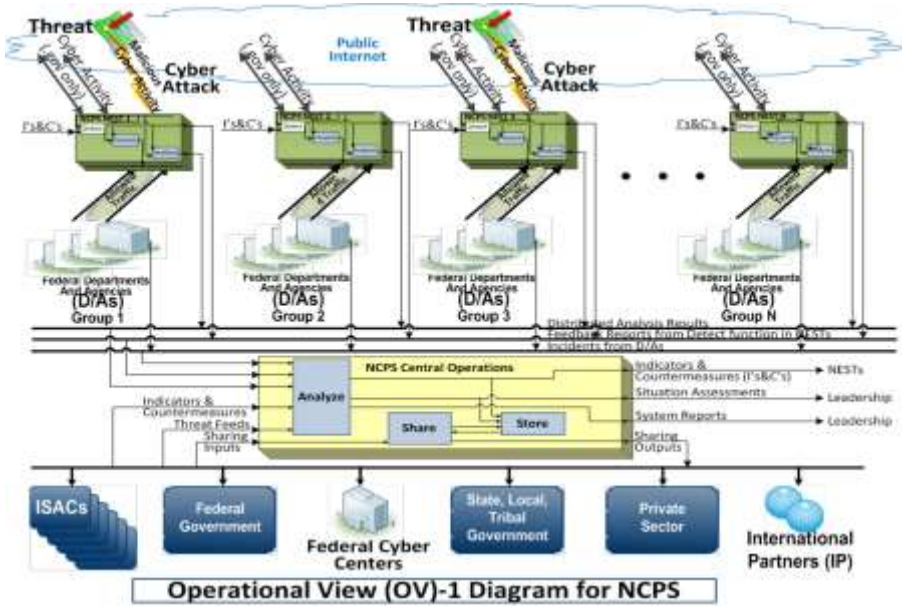
- Flexible platform for modeling, emulation, and controlled study of large, complex networked systems
  - USC/ISI (Los Angeles), UC Berkeley, and USC/ISI (Arlington, VA)
  - Funded by NSF and DHS, started in 2003
  - Shared resource – multiple simultaneous experiments subject to resource constraints
  - Open to academic, industrial, govt researchers
- Technical elements
  - Scalable Modeling and Emulation
  - Risky Experiment Management
  - Multiparty Experiments
  - Federation
  - Partner Cluster Deployment

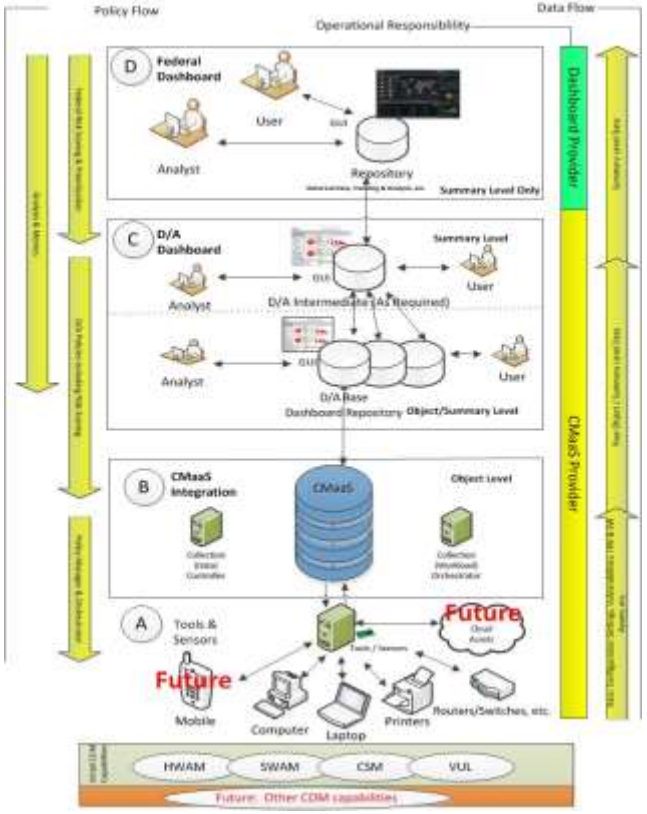
Homeland Security
Science and Technology

DHS Cyber Acquisitions



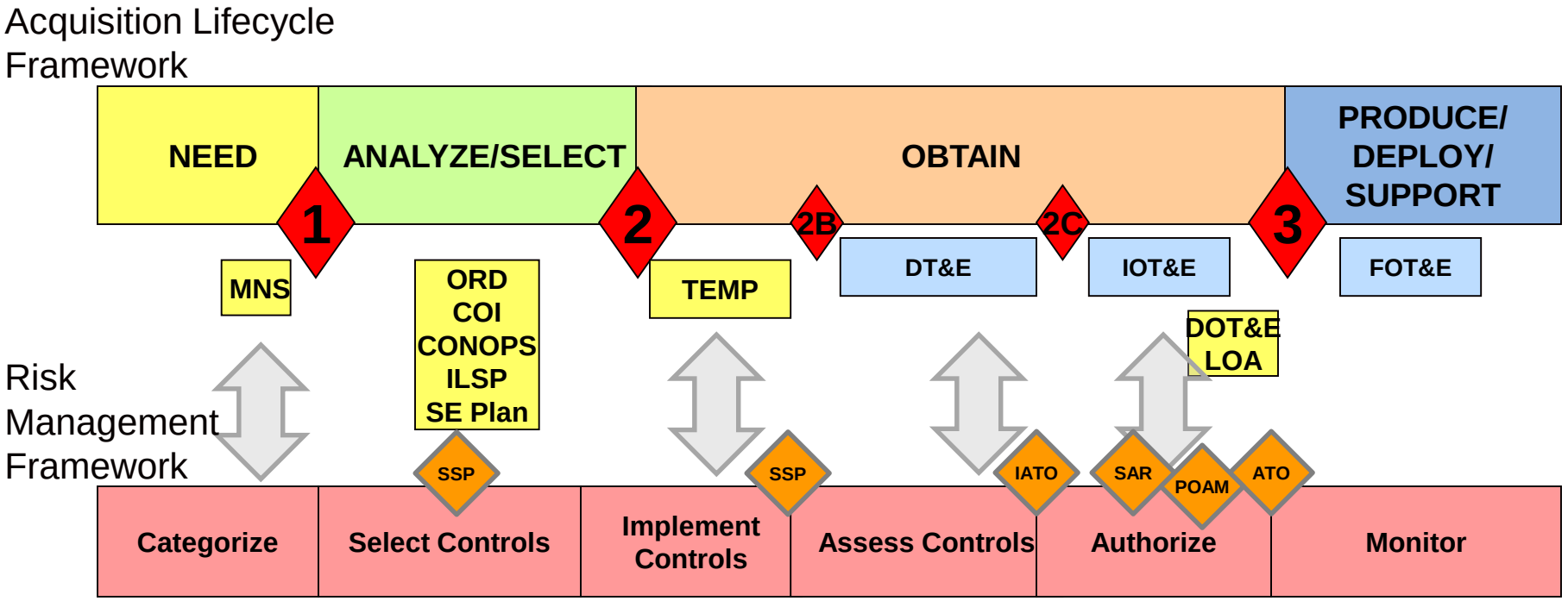
National Cybersecurity Protection System (NCPS)





Continuous Diagnostics Monitoring (CDM)

Cybersecurity in the Evaluation Framework



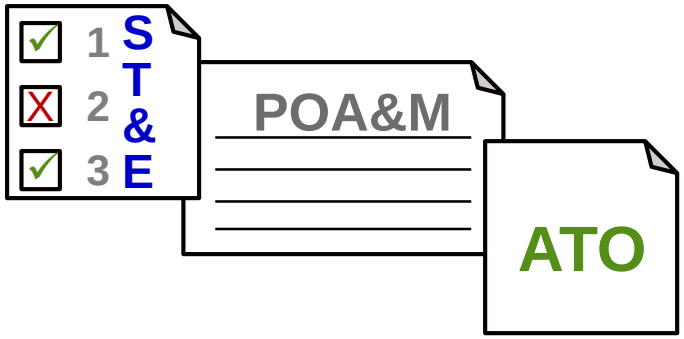
Cybersecurity Decision Support Questions

1. C1. Are cybersecurity requirements defined, measurable, and testable?
2. C2. Does the system software feature appropriate design-for-security elements?
2B. C3. Is there a sound plan to collect adequate cybersecurity data to inform production and deployment decisions?
2C. C4. Is the system sufficiently cyber secure to enter initial production?
3. C5. Is the system sufficiently cyber secure to enter full production/deployment?

Homeland Security
Science and Technology

T&E to Close the Gap

Authority to Operate



Homeland Security
Science and Technology

Questions?