Keynote Address

Teresa Takai
Chief Information Officer
U.S. Department of Defense
Cybersecurity – DoD CIO’s View
University of Rhode Island Cybersecurity Symposium

Teri Takai
Chief Information Officer
Department of Defense
May 2, 2013
Role of DoD CIO

- Ensure Defense of DoD Networks
- Work with our International partners to securely share information and collaborate on common norms of cyber defense
- Work with the Defense Industrial Base to Secure information vital to National defense
DoD is Big and Distributed

- People: More than 3.7 million; uniformed, civilian including guard and reserve
- Located in 163 countries
  - Facilities: “several hundred thousand buildings at more than 6,000 different locations...over 30 million acres of land”
... We Are Very Mobile ...

A USMC CH-53D on the flight deck of USS Tortuga off Ominato, Japan

A U.S. Navy EA-18G Growler takes off from Aviano Air Base, Italy
...and We Work With Many Expected and Unexpected Partners

- Allies and coalition partners
- Federal agencies
- State, local
- Industry partners
- Academia

- Most important DoD cybersecurity goal: Effective execution of military missions, even in the face of cyber warfare by a capable adversary.

2. Achieving mission assurance goes *beyond* hardening.

- Mission plans, networks, systems must be resilient in the face of successful cyber attacks.
- Design and planning of systems with this assumption – that sometimes hackers will succeed – supports this goal of resiliency.
3. We’ve got to achieve this mission assurance with our mission partners.

- Essentially every mission that DoD executes is completed with mission partners.

- This means that a DoD imperative is achieving mission dependability with whatever partners a mission requires.
4. Cyber resiliency must be designed and engineered.

- Redesign of DoD’s core information structure to Joint Information Enterprise will:
  - Empower cyber defenders to see, understand an entire “mission thread”
  - Make difficult or automatically dampen certain kinds of cyber attack
  - Allow “maneuver options” for cyber operators and defenders

5. Hardening, resilience, and sharing must go hand in hand.

- Sharing cannot be sacrificed to mission dependability.
- We have to do both.
6. Operational Cyber information sharing really works.

- Defense Industrial Base Cyber Security and Info Assurance program:
  - Successful DoD and DHS information-sharing program
  - Helps DIB companies stop theft of DoD info stored on DIB company systems
Final Lesson in Cyber Space

7. It is more about people than technology.

- The right workforce is still the most important part of cybersecurity.
- Every person who uses IT has a cyber responsibility.
- Everyone at DoD is trained on practicing good cyber hygiene and reporting suspicious behavior, incidents.
DoD Cyberspace Workforce: 6 Focus Areas

1) Establish cohesive cyberspace workforce policies
2) Employ multi-dimensional recruiting
3) Institutionalize continuous learning
4) Retain qualified personnel
5) Improve crisis and surge support
6) Expand threat knowledge & accountability
What does this mean to you?

- Cyber threats are real – How will you operate?
- Cyber Security means rethinking networks and information technology
- Information Security – Do you know who is on your networks?
- Information Sharing – Above / Across / Below
- Cyber Security is a cultural change
We’re Designing for Realistic Operational Environments

- Everything is connected to everything else
- We and our partners use IT for everything
- Potential adversaries understand this
In the end, addressing the cyber threat is a team sport across Federal, state, local government, academia, and industry.