Background

- TSA Information Assurance & Cyber Security Division (IAD) Cyber Security Awareness and Outreach (CSAO) Branch

- Mission:
  - Facilitate the measured improvement of the national transportation sector cyber security posture as both described and constrained by the National Infrastructure Protection Plan (NIPP), Homeland Security Presidential Directive -7 (HSPD-7), and modal private sector needs
    - Co-SSA with US Coast Guard for Maritime

- Branch Capabilities focused into four core competencies:
  - Education
  - Articulation
  - Coordination
  - Communication

- 2011 Branch Priorities:
  - Mitigating “Awareness as a Vulnerability”
  - Understanding and Communicating Common Risk
  - Enabling Better Information Sharing
What is Cyber Security?

- Webster: **Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack**

- What we think: **Systems are secure When they cannot be made to do more or less than their owners and society wish them to**
Cyber Security Threat is Real

- Cyber Attacks Today:
  - Active, targeted real life objectives, physical impacts, reasonable success rate

- Examples:
  - Stuxnet: Weaponized Malware with specific operational physical impact.
    - Targeted: Iranian Nuclear Program
  - HBGary: Expert Victims
    - Compromised by informal group of hackers using old, common techniques
    - Demonstrates that cyber security is hard to do effectively and reliably over time

- Realities:
  - Bad guys only need one way in: Defenders have to protect against them all
  - It’s safe to assume that someone can get in.
  - Attacker capabilities limited due to resources and motivation; not skill.
Where to start?

- It’s not just an IT or IT Security Responsibility
  - Recall the earlier definition of computer security?

- Owners, Executives, Operators are responsible for determining requirements and getting involved
  - You define the success criteria for cyber security
  - “Risks From Computer Systems”

- IT and IT Security staff responsible for engineering solutions
  - Address “risks to computers” which create the “risks from computers”
  - Within your appetite, other operational priorities, budget, etc.

- Collaboration needed on program and process components
What is TSA doing about it?

2011 Plans:

- Cyber Security Exercise
- Modal Outreach & Coordination
- Weekly Newsletter
- Summit 2011
- Strategy Development
- Information Sharing: Best Practices
- Facilitating/Aligning existing Government programs and efforts.

- All of the above accomplished through the TSSCWG
How can you get involved?

- Transportation Systems Sector Cyber Working Group (TSSCWG)
  - Critical Infrastructure Partnership Advisory Council (CIPAC) Chartered
  - 50+ members (Public and Private) and growing
  - Monthly Meetings – join us!

- Sign up for our weekly newsletter
- Attend our 2011 Cyber Security in Transportation Summit
Contact Information

- CyberSecurity@tsa.dhs.gov

- Kelley Bray
  Branch Chief, CSAO, TSA
  571-227-2198
  kelley.bray@dhs.gov