RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

DHS Cybersecurity Future Technology: Where We Go From Here

SESSION ID: ASEC-W04A

Brendan Goode

Director, Network Security Deployment
Department of Homeland Security

Overview

Our Engineering Vision

- Who We Are
- Building Future Engineering Capability
  - Where We've Been
  - Where We Are
  - Where We Are Going
- Final Thoughts

Who We Are

Network Security Deployment

- **Department of Homeland Security (DHS) and cyber mission:** Enhance the security, resilience, and reliability of the Nation’s cyber and communications infrastructure
- **Network Security Deployment (NSD) mission:** Design, develop, acquire, deploy, sustain, and provide customer support for the <u>National Cybersecurity Protection System</u>
- **National Cybersecurity Protection System (NCPS),** operationally known as EINSTEIN, provides key cybersecurity capabilities to defend against cyber threats targeted at Federal civilian government networks (.gov domain)

Building Future Engineering Capability

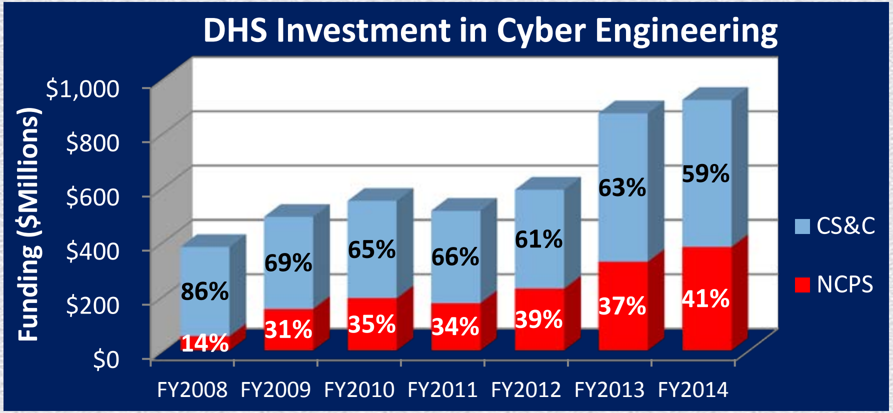
Where We've Been

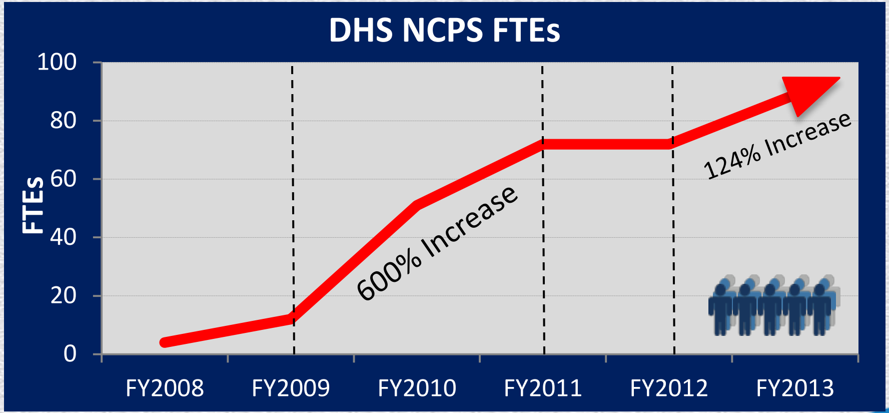
- In the mid-90s, the USG started to increase its focus on the cyber impact to critical infrastructure.
- After 9/11, the USG created institutions and organizations to resource the growing cyber challenge.
- The 2008 Comprehensive National Cybersecurity Initiative (CNCI) shifted government thinking about cybersecurity. In response, DHS evolved its execution strategy:
  - **Organizational:** Established a single engineering office and Program of Record in DHS
  - **Technical:** Determined that a scalable engineering and infrastructure capability was needed
  - **Architectural:** Focused on .gov & CI/KR stakeholders as part of a national solution

Building Future Engineering Capability

Where We Are: Capacity

- NCPS has created **engineering capacity**
  - **Investments**: Managing injection of seed capital in engineering infrastructure
  - **Human Capital**: Hiring team of engineers and specialists as part of human capital strategy
  - **Organizational Capital**: Creating management team and doctrine to support growth



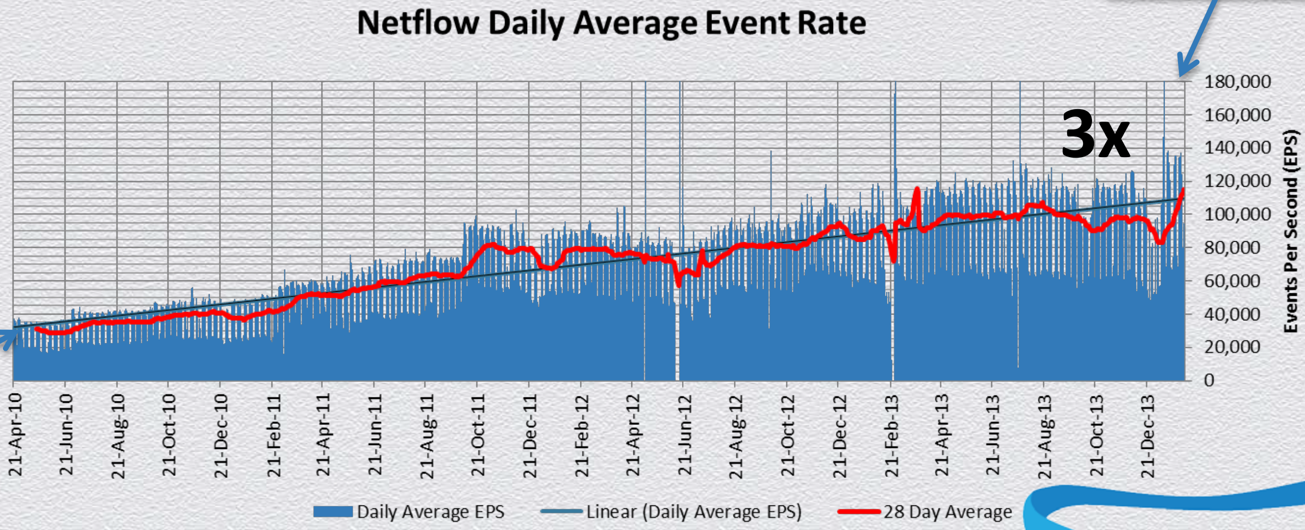


Building Future Engineering Capability

Where We Are: Capability

- NCPS fundamental **technical capabilities** in place for .gov customers
  - Intrusion Detection & Prevention
  - Integrated Analytics
  - Information Sharing
  - Infrastructure

~75 D/As covered



~12 D/As covered

Building Future Engineering Capability

Where We Are Going: Our Technical Vision

- **Engineering the right information, right people, right time, right manner:**
  - **Flexible**: Given the rapidly evolving threat, NCPS will focus on building a flexible, scalable infrastructure that can evolve at the “speed of threat”
  - **Innovative**: NCPS will integrate new capabilities and technologies quickly through pilots, test activities, and agile development approaches
  - **Responsive**: NCPS will accommodate integration of a community-based mindset into technology development
  - **Engaging**: NCPS will proactively partner with industry, academia, and other government entities

Final Thoughts

Focus on Common Engineering Goals

- Our Technical Vision draws heavily on smart engineering, creative integration, and new forms of partnership
- Stronger collaboration to address the toughest challenges:
  - Engineer cybersecurity to accommodate more powerful forms of technology
  - Deliver real-time situational awareness to large numbers of customers that have divergent needs, architectures, and business models
  - Create world-class engineering organizations

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

DHS Cybersecurity Future Technology: Where We Go From Here