Federal Cybersecurity Overview: Private and Public Partnerships

Leveraging Federal Cybersecurity and ISP Efforts to Benefit State and Local Governments

October 10, 2013

Raleigh Rhodes, CISSP, CPP
CenturyLink Government

CenturyLink™ Government

The Threat

Threat	Description	Threat Skill Level	Mitigation Effort
Nation State Sponsored	Nation states have targeted major governments and private industry around the world for espionage activities. Most US Federal Government organizations and many US industries have been targeted.	Advanced	Combating government sponsored adversaries require an advanced information security program. Even the most mature companies cannot completely stop these intrusions. Their goals are to reduce the time to detect the intrusion and develop indicators to stop similar attacks in the future.
Criminal Activity—Organized Crime	Moderate to sophisticated with well funded organized cyber crime syndicates.	Moderate to Advanced	Regulatory efforts for credit card, bank account and health care information protection have improved the overall security posture but is not adequate for advanced criminal attacks.
Hacktivism including Terrorism	Using computers and network infrastructure as a means of protest to promote political ends. This involves a wide range of activities from legal protests to destructive acts of cyber and physical resources.	Novice to Advanced	Most activity can be stopped through good information security practices. Recent destructive events have demonstrated more advanced capabilities.
Insider	Company employees pose a significant threat to a company's information security.	Novice to Advanced	Difficult to detect and stop. New content monitoring technologies and behavioral analysis systems can help identify & stop some malicious activity.

CenturyLink™ Government

Recent Cyber Attacks—Frequency and Scale

- August 2012—"Shamoon" Cyber Attack on world's largest oil producer—Saudi Aramco (Saudi Arabia)
  - Cyberattack results in physical destruction—**30K PC's hard drives wiped** and replaced image of burning U.S. flag
  - U.S. officials claim attacks were from Iran; retaliation for Stuxnet (2010 Nuclear shutdown) mentioned
- September 2012 & Continuing—DDoS attacks—Bank of America, Wells Fargo, JP Morgan Chase, US Bancorp, Citigroup, PNC, Capital One, and many others
- April 2013
  - **320+ Gbps DDoS attack—largest known published attack**
- April 23rd 2013—pro-Assad hacker group Syrian Electronic Army hacked into Twitter accounts for Associated Press
  - Spread false information that President Obama was injured at a bomb blast at the White House
  - Markets went into panic, DOW Jones sent plummeting by a staggering **$136 Billion**

CenturyLink™ Government

U.S. House Intelligence Committee—CISPA

- "The technological leadership and national security of the United States is at risk because some of our most innovative ideas and sensitive information are being brazenly stolen by these cyberattacks," stated House Select Intelligence Committee Chairman. Mike Rogers (R-Mich.)

Director of NSA and U.S Cyber Command Statement

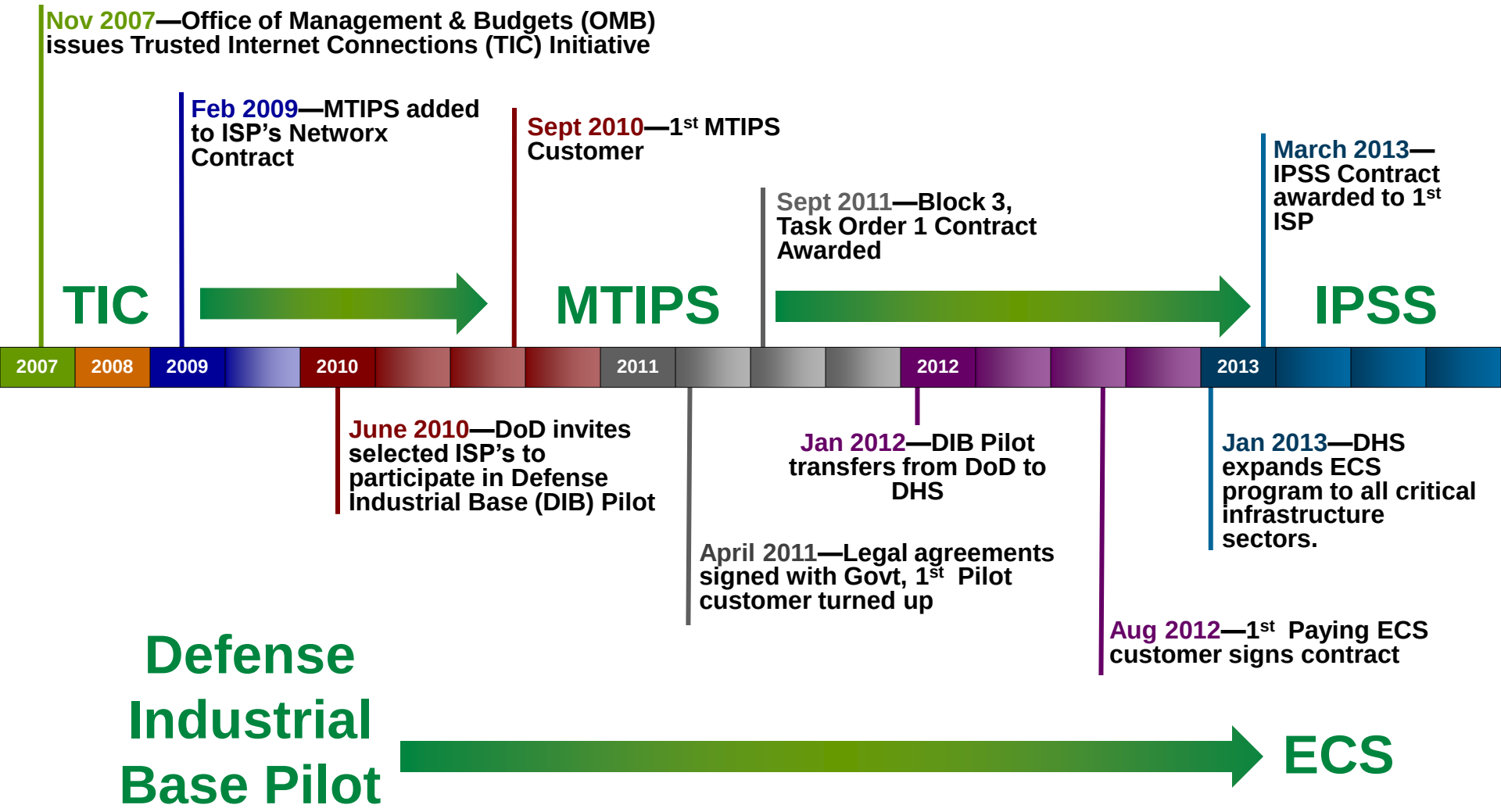
- According to General Keith Alexander, Director of NSA and U.S. Cyber Command, **"…cyberattacks are causing the greatest transfer of wealth in history."**
  - Crediting Symantec, the theft of intellectual property costs American companies up to **$300 Billion a year**
  - According to McAfee, the estimate the global cost of cybercrime is **$1 Trillion annually**
- General Alexander, while urging Congress to enact cybersecurity legislation to improve America's defenses stated, **"…That's our future disappearing in front of us."**

CenturyLink™ Government

Challenge for Every Agency IT Department

- Stopping the threat before it gets to their network edge
- Guaranteeing Confidentiality, Integrity and Availability of information systems and information assets.
- Ensuring operational continuity
- Preventing loss of thousands—sometimes millions—of dollars of value in lost productivity, lost revenue, lost customers—and diminished trust & reputation
- Relyiance on skill sets and/or technology not appropriate for the latest network-based threats
- Dedicating staff for security issues or allocating staff better suited to manage more strategic issues

ISP and Federal Cybersecurity Initiatives



CenturyLink™ Government

Federal Cybersecurity Initiatives & Programs

Internet Service Providers (ISP's) are engaged in a public/private partnership with the Federal Government to provide network based protections from nation-state attacks not available in the commercial space

- **Managed Security Services (MSS)**—A suite of traditional cybersecurity services provided via the GSA Networx contract.
- **Managed Trusted Internet Protocols Service (MTIPS)**—Via the GSA Networx contract, MTIPS facilitates the reduction of the number of Internet connections in Government networks and provides standard security services to Executive Branch government users.
- **Block 3 (B3)**—modified program provides program support, facilities and traffic aggregation for IPSS and ECS programs.
- **Intrusion Prevention Security Services (IPSS)**—provide protections for the US civilian federal government.
- **Enhanced Cybersecurity Services (ECS) - provide protections for critical infrastructure sectors including defense, banking & finance, energy, healthcare, and State, Local, and tribal Governments.**

CenturyLink™ Government

Managed Security Services (MSS)

- Traditional Network-based Security Services (network and premise based):
  - Managed Firewall
  - Intrusion Detection and Prevention
  - Managed E-Authentication
  - Vulnerability Scanning
  - Anti-Virus Management
  - Incident Response
  - Secure Managed Email
  - Managed Tiered Security
- Advanced Network-based Security Services
  - DDoS mitigation services

CenturyLink™ Government

MTIPS: Managed Trusted Internet Protocol Services

- Network Based Managed Security Services in a centralized ISP network location
- MTIPS 1.0
  - Managed Firewall Service
  - Email Scanning
  - Anti-Virus/Anti-Spam
  - Intrusion Detection Service (IDS)
- MTIPS 2.0 adds
  - Remote Access
  - Custom Remote Access
  - Extranet Connection
  - Custom Extranet Connection
  - Inventory mapping services

CenturyLink™ Government

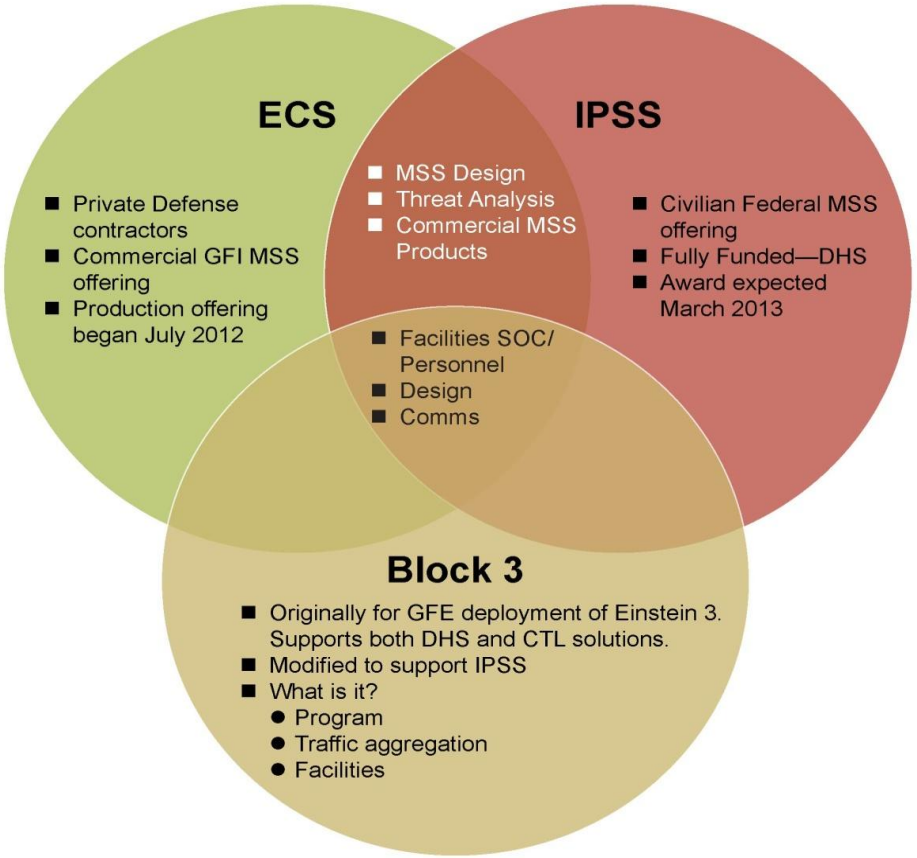
IPSS (E3A) Protections for U.S. Civilian Agencies

- Current Status
  - Only one ISP has received DHS IPSS IDIQ 4 year contract and Task Order 1 award to date; other awards pending
  - 2 Protection Measures (Advanced Email Filtering + DNS sinkholing)
  - Multiple Agencies currently operational
- Future Task Orders
  - Capacity for additional department and agencies (D/As)
  - Two protection measures + inline IPS capabilities
  - Additional security capabilities
  - Total civilian government coverage (all D/A's)
  - Full suite of protection measures (inline IPS capabilities)
  - By September 2015 systems will protect all ports and all protocols

CenturyLink™ Government

DHS and ISP Cybersecurity Program Interdependencies

Network based Managed Security Services (MSS)
- IPSS—Protections for Federal civilian agencies.
- ECS—Protections for approved critical infrastructure companies and **State, Local and Tribal Government**



NCPS (National Cybersecurity Protection System)—DHS Einstein monitoring .gov

"Block 1"—Trusted Internet Connection (TIC) with data flow sensors.

"Block 2"—Managed Trusted Internet Protocol Service with additional IDS capability.

"Block 3"—Originally, Government provided equipment housed in an ISP hosting facility. Replaced by ISP Managed Security Service using Government Furnished Information (GFI) and commercial indicators and technology.

CenturyLink™ Government

Enhanced Cybersecurity Services (ECS)

- Originally piloted for protection of private Defense Industrial Base (DIB) companies, program recently expanded to all critical infrastructure sectors
- Customers must be approved by DHS as an approved entity before receiving services
- State and Local Governments are included as part of the critical infrastructure that ECS is to protect
- Due to security and clearance requirements, ECS must be housed and managed in a Sensitive Compartmented Information Facility (SCIF). All personnel engaged must hold TS/SCI level clearances.
- ECS has transitioned from a Pilot to Production Service
  - Contracted customers - agreements signed
  - Expanding group of customers testing the service and entering into agreements
  - Critical Infrastructure sector companies are being identified and brought on to the ECS systems once approved by DHS and they have entered into an agreement for services

CenturyLink™ Government

ECS—Protection of All 16 Critical Infrastructure (CI) Sectors (**)

- **Defense Industrial Base**-current customer base (Lockheed Martin, Raytheon)
- **Financial Services** (Suntrust, Wells Fargo, PNC, Chase)
- **Energy** (Assoc of Oil pipelines, Duke Energy)
- **Healthcare and Public Health** (3M, Abbott, Kaiser, Inova)
- **Chemical** (BASF corp)
- **Commercial Facilities** (Marriott)
- **Communications** (CenturyLink)
- **Food and Agriculture** (Kraft, Conagra, General Mills)
- **Critical Manufacturing** (John Deere, GM, GE)
- **Dams** (Dominion, Duke Energy, Exelon Corp
- **Emergency Services** (Nat'l Sheriffs Assoc.)
- **Government Facilities** (State, local, tribal)
- **Information Technology** (Adobe, EMC, Dell, Sony, Symantec)
- **Nuclear Reactors, Materials and Waste** (Idaho Nat'l Lab, Covidien)
- **Transportation Systems** (Boeing, Truck Rental assoc.)
- **Water and Wastewater** (American Water)

*** Companies listed are Potential companies in each sector – DHS approval necessary*

CenturyLink™ Government

How can Enhanced Cybersecurity Services (ECS) Help Your State Cybersecurity?

Features

- Network-based inbound email filtering and neutralization targeting high impact, low volume threats not detectable using commercial threat signatures and solutions
- Advanced DNS protection and notifications – blocking of key malicious sites and disruption of command and control beaconing
- Advanced attack detection, prevention and mitigation
- Real time blocking, notifications and weekly reporting
- Multiple interface options to meet a variety of corporate email implementations
- Evolving security services provide state-of-the-art protections not available in commercial offerings
- Support provided 24/7/365 by Security Operations Center personnel

CenturyLink™ Government

DHS ECS Program website

http://www.dhs.gov/enhanced-cybersecurity-services

CenturyLink™ Government

Questions

Thank you.

Raleigh Rhodes
CenturyLink Government

The CenturyLink Government ECS team can be reached by sending an email to:
ecs@centurylink.com

CenturyLink™ Government