DHS SCIENCE AND TECHNOLOGY

AIMS Presentation

Homeland Security

Science and Technology

April 17, 2019

Ann Cox

Program Manager

Physical and Cybersecurity Division

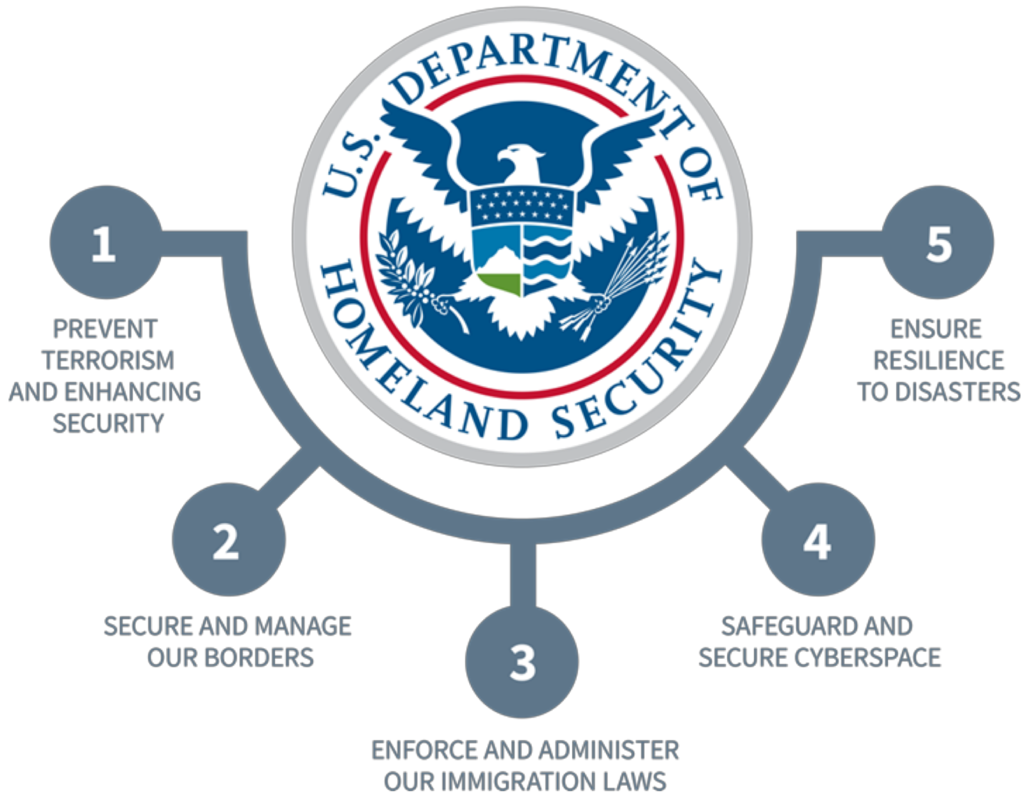
S&T in Brief

- **~ 1,200 personnel**
  - Federal, Contractor, IPAs, highly technical staff
- **Laboratories**
  - 5 internal Labs, 2 Federally Funded R&D Centers, access to DOE Labs
- **Centers of Excellence**
  - Network of university-based COEs
  - Multidisciplinary research and education in homeland security-related fields
- **Collaborates across sectors to develop, leverage, transition capabilities**
  - Components, State/Local, Interagency, International, Private Sector, Academia
- **Supports DHS, Components and HSE requirements**
  - Key technical and analytical capacity in major threat areas
  - Innovative approaches to problem solving and affordable, viable solutions
- **Establish enduring capability in homeland security science and technology**
  - Prepare future generations to meet homeland security challenges

S&T MISSION

Enable effective, efficient and secure operations across all homeland security missions by applying scientific, engineering, analytic and innovative approaches to deliver timely solutions and support departmental acquisitions.

DHS FIVE MISSION AREAS



1 PREVENT TERRORISM AND ENHANCING SECURITY

2 SECURE AND MANAGE OUR BORDERS

3 ENFORCE AND ADMINISTER OUR IMMIGRATION LAWS

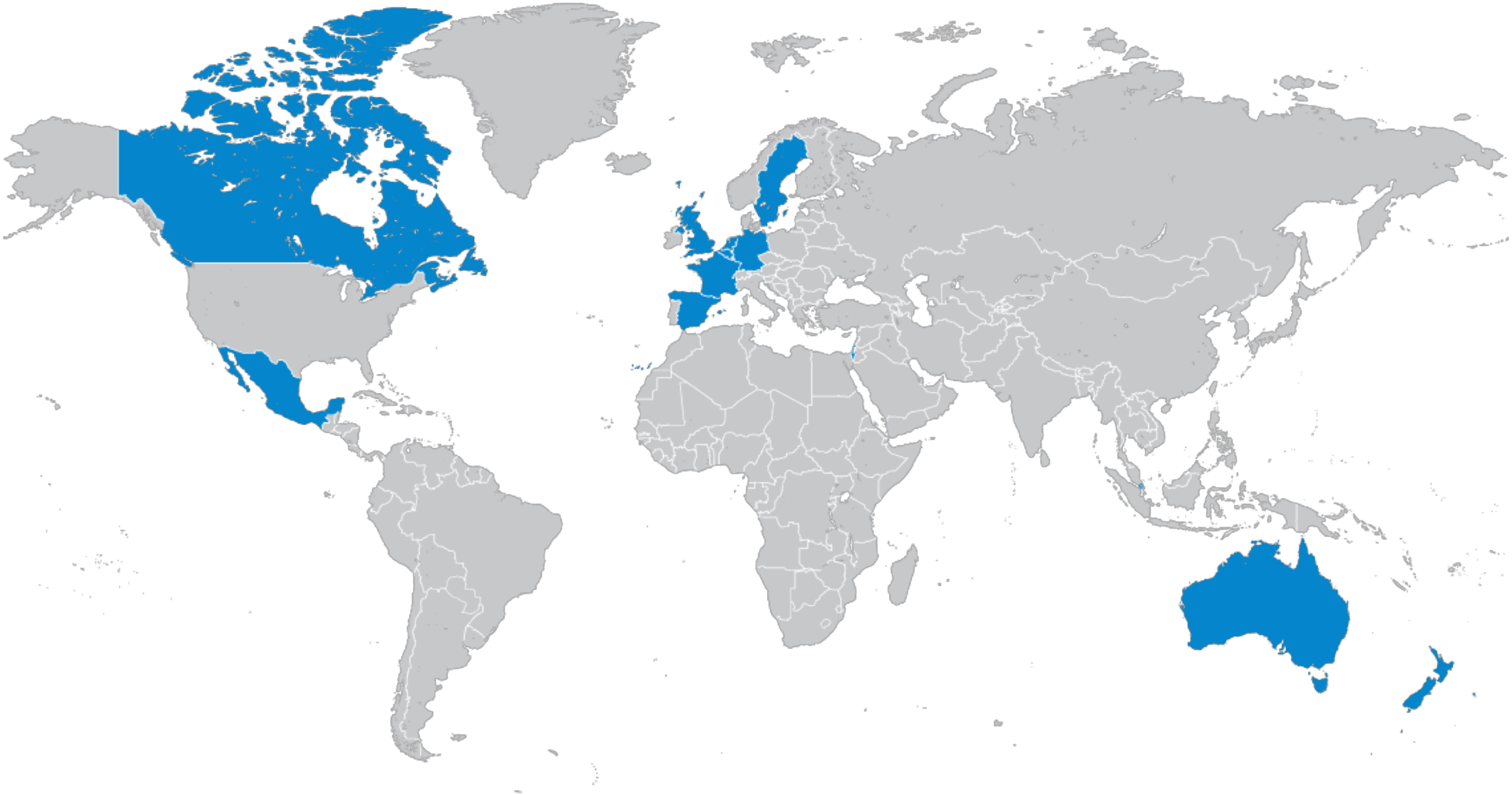
4 SAFEGUARD AND SECURE CYBERSPACE

5 ENSURE RESILIENCE TO DISASTERS

INTERNATIONAL PARTNERSHIPS

S&T develops partnerships with foreign governments and international organizations to enhance scientific and technical knowledge for the global Homeland Security Enterprise.

- Australia
- Canada
- France
- Germany
- Israel
- Mexico
- Netherlands
- New Zealand
- Singapore
- Spain
- Sweden
- United Kingdom
- European Commission



Doing Business with S&T

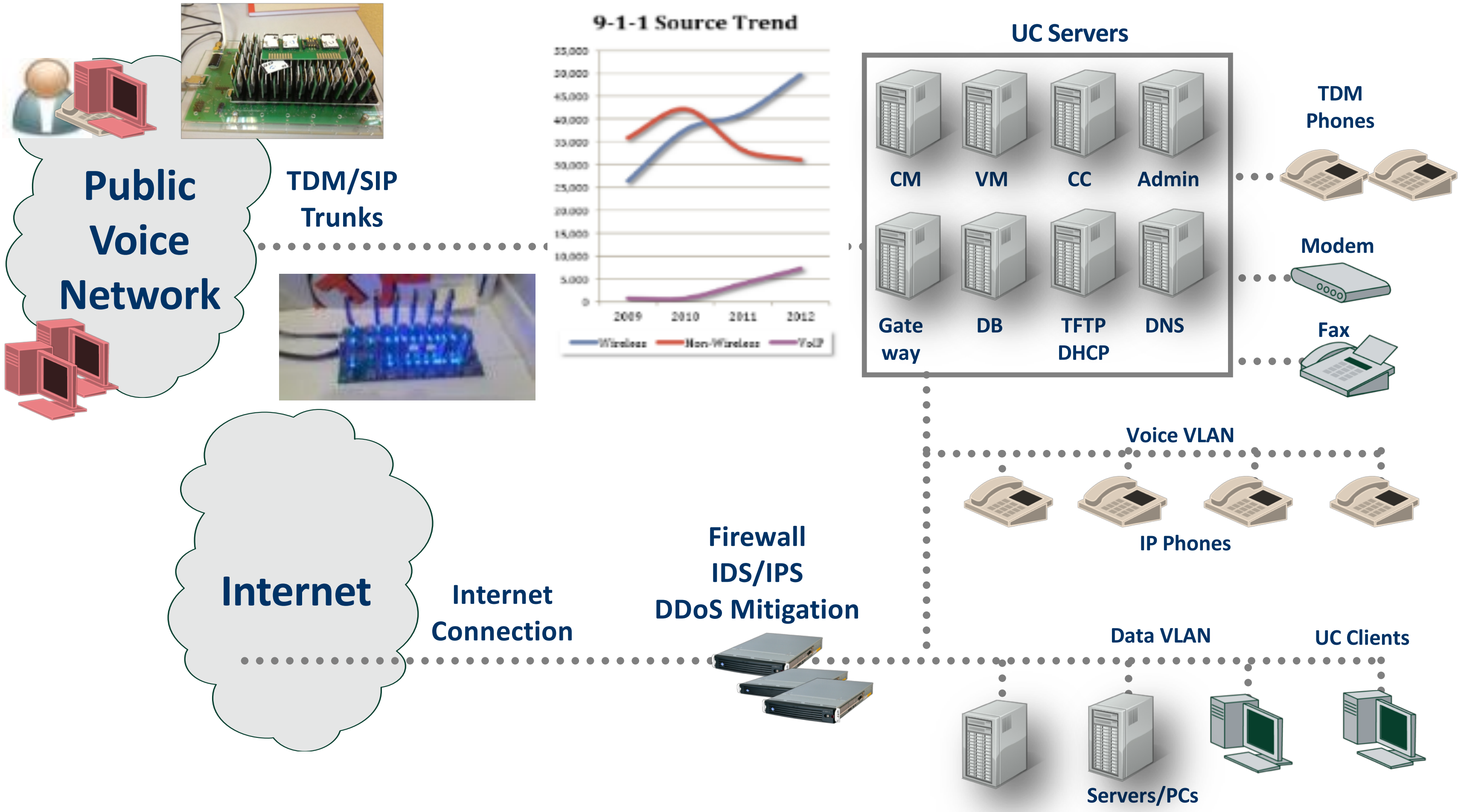
S&T seeks to engage innovators and a wide variety of performers to develop science and technology solutions that address real-world threats and hazards.

- **Silicon Valley Innovation Program** – engages technology innovators and investors to solve pressing homeland security challenges
- **S&T's Long Range Broad Agency Announcements** – open invitation to scientific and technical communities to fund pioneering R&D projects
- **S&T's Small Business Innovation Research Program** – awards funds to small businesses to quickly commercialize and deliver operational prototypes
- **Prize Competitions** – incentivizes non-traditional performers to propose innovative solutions
- **SAFETY Act** – offers important legal liability protections for providers of Qualified Anti-Terrorism Technologies
- **Transition to Practice Program** – helps federal laboratories and research centers transition promising solutions for commercialization

DDoS TDoS

- Problem statement/capability need summary
  - Distributed Denial of Service (DDoS) Attacks have disrupted government, critical infrastructure, and key communications systems.
  - Government leadership is needed to promote the use of existing best practices that eliminate some types of DDoS attacks and make it easier to counter other types of attacks.
  - A requirement exists to develop tools and techniques to protect the Internet resources of aa medium scale organization such as a government agency, medium scale bank, or dam, power utility, or other infrastructure control system.
  - A requirement exists to develop defenses for critical communications systems that are rapidly becoming connected to the Internet and thus vulnerable to new types of Telephony Denial of Service attacks (TDoS).
- Describe alignment with higher level guidance
  - This work focuses on providing a trusted cyber future. DDoS attacks remain one of the most widely used forms of attack and continue to disrupt both government networks and critical infrastructure sectors. No one organization or vendor can solve the problem on their own.
  - This work addresses emerging problems in securing communications for first responders, especially for 911 systems.
- Identify the impact of not making this improvement or adding the new technology
  - Several prominent DDoS attacks have disrupted government, journalists, and industry. These attacks will only grow larger and defenses to address large attacks will not keeping with advances in attacks unless government acts to promote DDoS defense.
  - Errors and attacks have disrupted 911 systems and have resulted in loss of life for US citizens. The scale of attacks threaten to increase dramatically. In 38 states, no money was spent in 2015 on cyber security for 9-1-1 centers and only 420 out of 6,500 9-1-1 centers had implemented a cyber security program.

TDoS Threat –Disable 911



DDoS

USC-ISI SENS

- Enables any ISP to offer automated services for DDoS diagnosis and mitigation
  - Secure, robust to misbehavior
  - Software solution, works with existing ISP infrastructure

University of Oregon, Drawbridge

- Will enable users to inform ISPs how to handle DDoS attacks. On attack, the user generates and sends DDoS-filtering rules to the DrawBridge controller at an upstream ISP. The controller verifies and deploys the rules at well-chosen switches or ISPs to filter DDoS traffic

Colorado State University – Netbrane

- Automated, distributed DDoS detection and mitigation in minutes

TDoS

Securelogix - A Layered Service Provider/customer Approach to Call Spoofing/TDOS

- Detect calling number spoofing, authenticate number.
- Authenticate device assigned to number, not caller
- Leverage collaboration with major carriers, providing an API for greater network visibility

AnaVation LLC - Verification of Caller Ascertained Logically (VOCAL)

- The Do Not Spoof Service (DNSS), a modular, componentized solution for spoofed call detection and blocking and/or notification via multi-layered call and user authentication and validation. Detects spoofed calls and either blocks them or notifies the victim and other relevant parties

Illuma Labs - Real-time Authentication to counter Caller ID Spoofing

- Real-time ‘Authentication as a Service’ to secure telephone communications
- Lightweight client supporting resource constrained platforms (e.g. smartphones)
- First caller authentication solution available outside call centers (e.g. mobile, laptops)

Software Assurance

Problem Statement

- An increasing amount of our nations critical infrastructure and economy are dependent on software driven systems
- The complexity of software is increasing (e.g. increased computing at the edge, autonomous systems, integration from multiple sources)
- Approximately 84% of recorded software breaches exploit vulnerabilities at the application layer1
- Software Assurance testing can be a manual, time intensive process and the cost to correct deficiencies increases later in the software development life cycle

Describe alignment with higher level guidance

- Software assurance research directly relates to elements of the 2018 National Cyber Strategy and the DHS Cyber Security Strategy, specifically securing Federal networks and information and protecting Critical Infrastructure
- The adoption of software quality assurance techniques through broader education supports the development of a cybersecurity workforce life cycle

Identify the impact of not making this investment

- Software assurance tools and techniques will not keep pace with the continued growth and complexity of software
- Wider adoption of software assurance tools and techniques will be impeded

Sources:

1) Niddifer, Woody, Chick: Program Manager's Guidebook for Software Assurance, Dec 2018, CMU-SEI

Software Assurance

Secure Decisions - Application Security Technologies & Metrics (ASTAM): Faster testing and better vulnerability coverage through automation

- Technologies that automate some of the most labor-intensive and difficult processes of Application Security
  - Penetration testing
  - Threat modeling
  - Research and development of AppSec metrics and reports

IUPUI - Classifying False Positives Generated By Static Code Analysis Tools

- Use code reduction techniques (e.g., delta debugging) to reduce error generating code to the smallest snippet of code required to generate a false positive.

Grammatech - Static Tool Analysis Modernization Project (STAMP)

- Bug-Injector tool (DARPA SBIR and STAMP) automatically generates realistic test cases
  - Injects bugs for a desired CWE into a desired host program
  - Large, complex test programs allow stress-testing of tools
  - Automated generation technique
  - reduces test suite bias

Morgridge Institute for Research - Software Assurance Marketplace (SWAMP): Continuous Assurance

- Through the SWAMP's open, continuous software assurance framework, there are two ways to bring continuous assurance capabilities to the developer community:
  - SWAMP is a ready-to-use open facility located at mir-swamp.org.
  - SWAMP-in-a-Box is an open distribution of SWAMP software available for download on GitHub or swampinabox.org.

Sources:

1) **Niddifer, Woody, Chick: Program Manager's Guidebook for Software Assurance, Dec 2018, CMU-SEI**

Application of Network Measurement Science – PARIDINE

Predict, Assess Risk, Identify (and Mitigate) Disruptive Internet-scale Network Events

Problem Statement

- The internet is vast and extremely difficult to “monitor”. Although many efforts to make individual measurements exist, they are limited in scope, and cannot detect or communicate Network/Internet Disruptive Events (NIDEs) until the event has already occurred.
- The measurement and monitoring that currently takes place is
  - Government level, may be classified data
  - Private Sector, proprietary data
  - Academic, limited in scope

Advantage Favors Chaos

- Resources Costs Favor Attackers
- Attacks require fewer resources because they can be narrowly focused, whereas defenders must spread resources to cover all attack surfaces. The size and scope of the internet allows small malicious actions to go undetected
- Problems may be caused by deliberate or accidental events, or as an unintended consequence of some other benign effort
  - May exploit unknown vulnerabilities
  - Will not be anticipated through monitoring
- Proprietary networks and a highly competitive environment discourage information sharing and broad based defense
  - The development of systems to identify, monitor, attribute, and communicate NIDEs will encourage best practices and allow for a more uniform resiliency

Application of Network Measurement Science – PARIDINE

Predict, Assess Risk, Identify (and Mitigate) Disruptive Internet-scale Network Events

CAIDA, University of California, San Diego - Ioda-NP: Multi-source Realtime Detection of Macroscopic Internet Connectivity Disruption

- Capable of detecting large-scale events of connectivity disruption in near-realtime.

University of Southern California, Information Sciences Institute - Detecting, Interpreting, and Validating from Outside, In, and Control, disruptive Events (DIVOICE)

- Definitions, detection methods, and systems that provide:
  - Network outages: measured with Trinocular (outside-in) and Disco (inside-out)
  - Routing anomalies: hijacks and detours with BGPMon

University of Waikato, New Zealand - Recording Router Reboots for Rating Router Reliability and Reachability

- Fine-grained active probing of routers to identify when a router has restarted, and then (1) examine the effect that reboot had on prefix reachability in the Border Gateway Protocol (BGP) routing system, and (2) examine the effect that reboot had on the reachability of systems the router was on the path towards.

Two Six Labs - Attribution and Recognition of Characteristics Underlying Scenarios (ARCUS) with NIDEs

- Near-real-time identification and causal attribution of NIDEs through a scalable, machine-learning-based system that fuses information from multiple Internet telemetry sensor arrays.

Securelogix - Detecting Disruptive Call Events In 9-1-1 and Communication Networks

- Gathering data from existing 9-1-1 environments to enhance machine learning models that are the basis of cloud-based Call Authentication Service (CAS).

Engage With Us!

WEBSITE
scitech.dhs.gov

PERISCOPE
periscope.tv/dhsscitech/

TWITTER
@dhsscitech

YOUTUBE
youtube.com/dhsscitech

FACEBOOK
@dhsscitech

FLICKR
flickr.com/photos/dhsscitech/

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS