



Cyber Security Division

FY 2013 Annual Report



**Homeland
Security**

Science and Technology

CYBER SECURITY DIVISION

FY 2013 ANNUAL REPORT



LETTER FROM THE DIRECTOR

Douglas Maughan, Ph.D.

Today, our economic strength and national security relies heavily on a vast array of interdependent and critical networks, systems, services, and resources to conduct daily business decisions and transactions. The assets that we rely on are being threatened frequently by cyberattacks. In support of the Department of Homeland Security Science and Technology Directorate's (S&T) mission, the S&T Cyber Security Division (CSD) develops and delivers new cybersecurity research and development (R&D) technologies, tools, techniques, and next-generation cybersecurity capabilities to enable the department and our nation to defend, mitigate, and secure current and future systems and networks against cyberattacks.

Improvements in cybersecurity, a global issue, depend on international public-private partnerships. In 2013, we continued building those bridges through cybersecurity research engagements with the Australia, Canada, Japan, the Netherlands, Sweden, and the United Kingdom in areas such as cyber economic incentives, software assurance, and modeling of Internet attacks. In addition to CSD's investment, our international partners have invested more than \$6 million in joint funding across 33 of our projects to improve the cyber landscape.

Technology transition continues to be an essential goal of the division, allowing our impact to extend to our operational partners in the government and private marketplace. During fiscal year 2013 (FY 2013), CSD had a number of successful pilots and deployments across the Homeland Security Enterprise. For example, our Software Quality Assurance project piloted CodeDx—a technology that visualizes and correlates outputs from disparate code analysis tools and puts them into the proper context for effective triage and

mitigation—with the State of Pennsylvania. We also deployed Blackthorn3, a manufacturer-agnostic GPS forensics tool that automates the collection of evidence from GPS devices, through our Cybersecurity Forensics project.

In FY 2013, CSD focused efforts to address Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience. The implementation of these policies has emphasized the need for holistic teamwork in security and risk management and the need to enhance the efficiency and effectiveness of the U.S. government's work to protect and secure critical infrastructure. As a subset of these orders, CSD was tasked to lead the development of the National Critical Infrastructure Security and Resilience (CISR) R&D plan. The development of the plan has taken into account the evolving threat environment and annual metrics to identify priorities to guide federally funded R&D requirements and investments. The plan is leveraging existing plans and we are incorporating other EO/PPD deliverables into the CISR R&D Plan. Although a lot of progress has been made, the plan will not be released until early 2015.

In addition to our international partnerships, pilots and deployments, and EO/PPD efforts noted above, this FY 2013 Annual Report will cover many other accomplishments across our portfolio. I'd like to point out a few of these highlights:

- Our **Identity and Access Management** project continues to share best practices with more than a dozen federal, state, local, and regional working group participants; demonstrate the operational capability of identity and access management at the Washington, D.C. Office of the Chief

Technology Officer; provide a testbed to explore and evaluate identity, credentialing, and access management architectures; and mitigate the risk for operational use by developing proof-of-concept solutions.

- The **Network and Systems Security** program has provided operational and beta tools to detect and analyze Internet traffic under the Internet Measurement and Attack Modeling project and a Secure Cloud Computing project that started an effort to automatically detect, evaluate, and mitigate cloud-specific security risks.
- Our **Transition to Practice (TTP)** project is bridging the technology transition “valley of death” by identifying federally funded technologies with great potential, promoting them through demonstration and outreach, and connecting these technology developers with commercialization partners. TTP demonstrated eight technologies in FY 2013 and identified an additional nine technologies to be demonstrated in the future.
- The **Domain Name System Security (DNSSEC) Extensions Deployment Initiative** project was successfully completed in FY 2013. DNSSEC provides security for a critical piece of the Internet’s infrastructure. It has been deployed in 85 percent of U.S. government websites and the project was transitioned to the Internet Society’s Deploy360 Programme to manage and continue the deployment effort across the broader Internet.

Looking into FY 2014, we will be wrapping up funded efforts and receiving final deliverables from the Broad Agency Announcement 11-02 in Internet Measurement and Attack Modeling, Moving Target Defense, Software

Assurance, Tailored Trustworthy Spaces, and Usable Cyber Security topic areas. The first set of technologies selected for the TTP project will participate in their final demonstrations, presenting to the private sector community in anticipation that each technology could be chosen for commercialization. As existing projects end, new projects such as Mobile Technology Security and Cyber Physical System Security will be added to our portfolio.

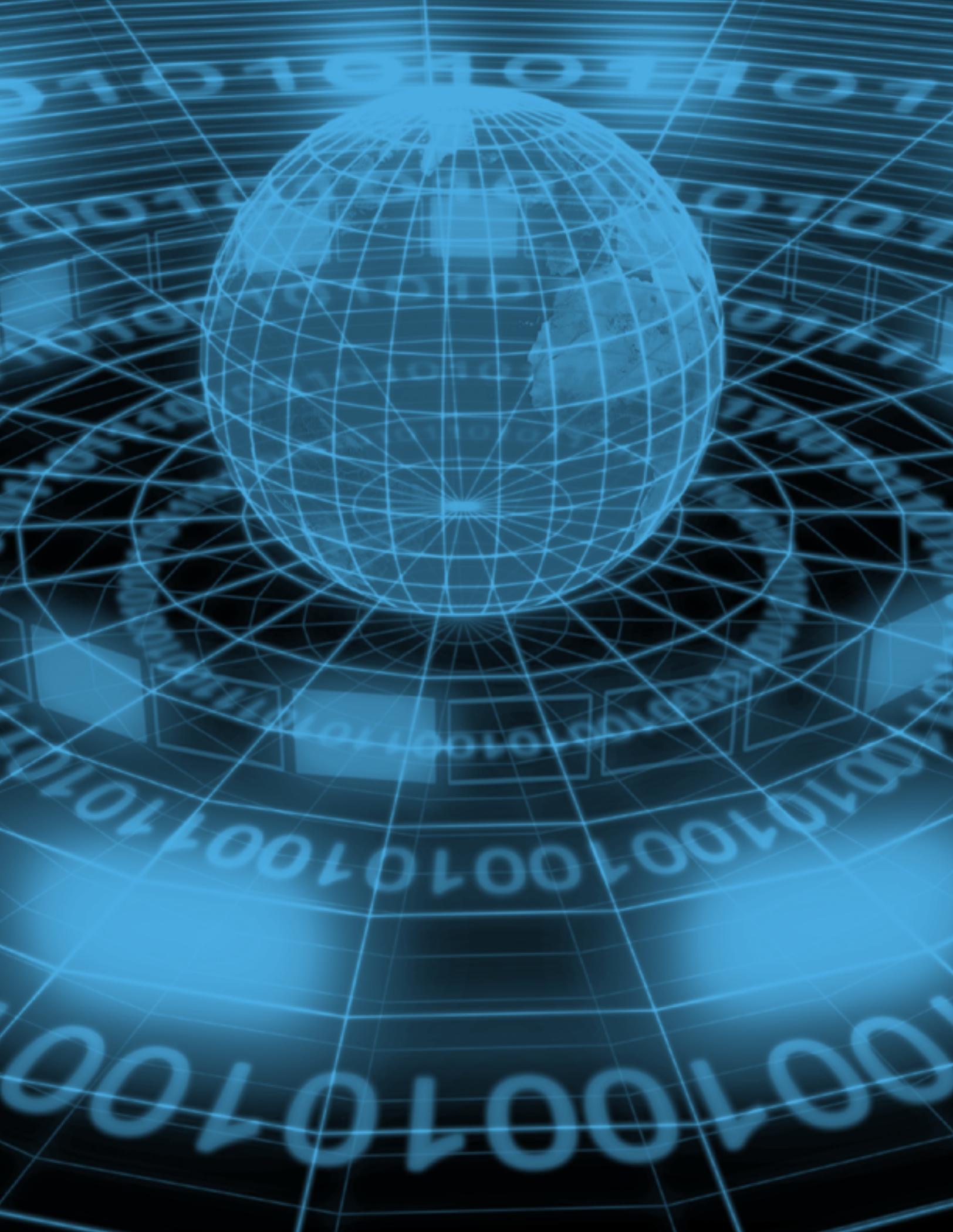
Finally, we will continue our outreach and transition efforts with the public and private sector to help us gather requirements and identify partners to improve our ability to develop new tools and technologies to secure and protect our nation’s systems and networks.

For additional information, please visit our website at www.dhs.gov/cyber-research, follow us on Twitter at @dhsscitech, or reach out directly to the CSD program managers listed in this report.



Douglas Maughan, Ph.D.

Cyber Security Division Director
Department of Homeland Security
Science and Technology Directorate



CONTENTS

II	LETTER FROM THE DIRECTOR
2	CYBER SECURITY DIVISION OVERVIEW
4	IDENTITY MANAGEMENT AND PRIVACY
6	Data Privacy Technologies
8	Identity and Access Management
10	LAW ENFORCEMENT SUPPORT
12	Cybersecurity Forensics
14	NETWORK AND SYSTEMS SECURITY
18	Mobile Technology Security
20	Internet Measurement and Attack Modeling – Network Mapping and Measurement
22	Internet Measurement and Attack Modeling – Modeling of Internet Attacks
24	Internet Measurement and Attack Modeling – Resilient Systems and Networks
26	Secure Cloud Computing
28	Moving Target Defense
30	Tailored Trustworthy Spaces
32	Enterprise Level Security Metrics
34	Insider Threat
36	RESEARCH INFRASTRUCTURE
38	Experimental Research Testbed
40	Research Data Repository
42	SOCIAL-BEHAVIORAL EDUCATION, LEARNING, AND TRAINING
44	Useable Cybersecurity
46	Cyber Economics Incentives
48	Cybersecurity Competitions
50	Incident Response Communities
52	SOFTWARE ASSURANCE
54	Software Quality Assurance
56	Software Assurance Marketplace
58	TRUSTWORTHY INFRASTRUCTURE
62	Trustworthy Cyber Infrastructure for the Power Grid
64	Secure Protocols for the Routing Infrastructure
66	Linking the Oil and Gas Industry to Improve Cybersecurity
68	Domain Name System Security Extensions Deployment Initiative
70	Distributed Environment for Critical Infrastructure Decision Making Exercises
72	TRANSITION AND OUTREACH
74	Transition to Practice
76	Experiments and Pilots
78	Cybersecurity Assessment and Evaluation
80	Homeland Open Security Technology
82	PERFORMER INDEX



CYBER SECURITY DIVISION OVERVIEW

The mission of the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cyber Security Division (CSD) is to:

- Develop and deliver new technologies, tools, and techniques to enable DHS and the United States to defend, mitigate, and secure current and future systems, networks, and critical infrastructure against cyberattacks;
- Conduct and support technology transition and approaches across the Homeland Security Enterprise; and
- Lead and coordinate research and development (R&D) among DHS components and customers, other government agencies, academia, private sector, and international partners within the cybersecurity R&D community.

CSD's mission directly supports the Quadrennial Homeland Security Review, Mission 4: Safeguard and Secure Cyberspace by helping to create a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation. To accomplish this mission, CSD closely collaborates with a wide range of partners across DHS, federal agencies, state and municipal administrations and first responders, critical infrastructure sectors, global Internet governance bodies, cybersecurity researchers, universities, national laboratories, and international organizations on multiple cybersecurity projects. CSD has organized its work into eight major program areas.



IDENTITY MANAGEMENT AND PRIVACY:

Develops cost-effective technologies for identifying individuals and managing their access to resources and data.



LAW ENFORCEMENT SUPPORT:

Ensures the nation's law enforcement has the most up-to-date investigation tools and techniques to combat criminal and terrorist activities.



NETWORK AND SYSTEMS SECURITY:

Develops tools for improving the security and protection of user online activity.



RESEARCH INFRASTRUCTURE:

Provides a research infrastructure to enable the national and international cybersecurity research community to discover, test, and analyze state-of-the-art tools, technologies, and software in a scientifically rigorous and ethical manner.



SOCIAL-BEHAVIORAL EDUCATION, LEARNING, AND TRAINING:

Focuses R&D activities on the human elements of cybersecurity such as technology usability, incentives, and behavioral analysis.



SOFTWARE ASSURANCE:

Develops tools for improving vital software used by government, businesses, and critical infrastructure owners and operators.



TRUSTWORTHY INFRASTRUCTURE:

Ensures that the nation's critical infrastructure—such as the power grid, oil and gas pipelines, and the banking and finance sectors—become more secure and less vulnerable to malicious and natural events.



TRANSITION AND OUTREACH:

Provides an accelerated transition path of new and existing cybersecurity technologies, including open-source solutions, into commercial products and services.



IDENTITY MANAGEMENT AND PRIVACY

As Internet usage continues to grow, users find it increasingly difficult to protect their personal information and trust the security and identity of online resources when sharing information. To address this, the Identity Management and Privacy program is developing fundamental technologies for identifying individuals and managing their access to resources and data. These cost-effective technologies will address security risks, increase productivity, and ensure personal information is used appropriately and with minimal risk to privacy.

In fiscal year (FY) 2013, CSD carried out the Identity Management and Privacy program through two projects.

DATA PRIVACY TECHNOLOGIES

As the amount of personally identifiable information (PII) that is collected and used increases, it is becoming more difficult to secure the data. CSD is developing technologies to help organizations responsibly manage PII in a manner that protects individual privacy.

IDENTITY AND ACCESS MANAGEMENT

In many organizations, the ability to share information securely and effectively has diminished due to inadequate enforcement of security policies and procedures. CSD is researching and developing identity management technologies to enable seamless and secure interactions among federal, state, local and public private sector organizations.



DATA PRIVACY TECHNOLOGIES

CSD initiated a research and development project seeking to secure PII based on needs of the Homeland Security Enterprise (HSE) to secure privacy. The Data Privacy Technologies project is developing a set of technologies to help organizations responsibly and safely manage personal information, maintaining individuals' privacy in accordance with laws and policies. Such tools are critical enablers of information sharing as they foster confidence that personal information is being used appropriately while minimizing privacy risks.

CSD is supporting the application of privacy technology to HSE's missions by exploring, refining, and integrating technologies and techniques and piloting the results. CSD is identifying and prioritizing specific DHS privacy technology needs through the S&T Privacy Working Group, which is comprised of privacy stakeholders including the DHS Privacy Office, and various DHS components. Additional members from fusion centers, state and private sector organizations are considered on a case-by-case basis depending on their operational-level view of privacy gaps in the HSE. The Privacy Working Group meets annually or as needed, so CSD may gather requirements to address common capability gaps.

S&T is collaborating with federal, state, local, and private sector organizations to enhance information sharing mission needs. Research projects entail a full lifecycle procedure including the following project:

- Gather mission requirements related to protecting PII from intelligence analysts in Fusion Centers.
- Develop automated processes for intelligence analysts and fusion centers to securely share information and ensure compliance with intelligence oversight legislation and privacy regulations. The developed tools provide analysts information in order to make timely, informed decisions before sharing information.
- Provide tools for authorizing sensitive information to be shared across domains and jurisdictions. These tools will automate compliance with PII laws and policies, eliminating human errors associated with the manual processes currently being used.



FY 2013 HIGHLIGHTS

- Program Manager Karyn Higa-Smith presented the CSD Data Privacy initiative at the Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy (video at <https://www.youtube.com/watch?v=fzkAtfx6W-g&feature=youtu.be>).
- Research performer (Massachusetts Institute of Technology) presented at the 2013 IEEE International Conference on Technologies for Homeland Security on the development and integration of the Policy Reasoning Engine with the Backend Attribute Exchange standard for user attributes.



PERFORMERS

- Massachusetts Institute of Technology
- The MITRE Corporation



PROGRAM MANAGER

Karyn.Higa-Smith@st.dhs.gov



IDENTITY AND ACCESS MANAGEMENT

The identity management challenge begins with answering the questions: are you who you claim to be and are you authorized to be here? Trust in the answers to those questions requires secure, interoperable, and efficient methods. Agencies and organizations lack the infrastructure and technologies needed to share and coordinate information effectively—not because of inadequate data and information sharing environments, but because of inadequate security, trust, usability, procedures, and policy enforcement.

TTWG PARTICIPANTS

- All Hazards Consortium
- Chester County, PA
- Colorado
- District of Columbia
- Florida
- Maryland
- Missouri
- Nevada
- Pennsylvania
- Pittsburgh, PA
- Rhode Island
- Southwest Texas
- Texas
- Virginia
- West Virginia

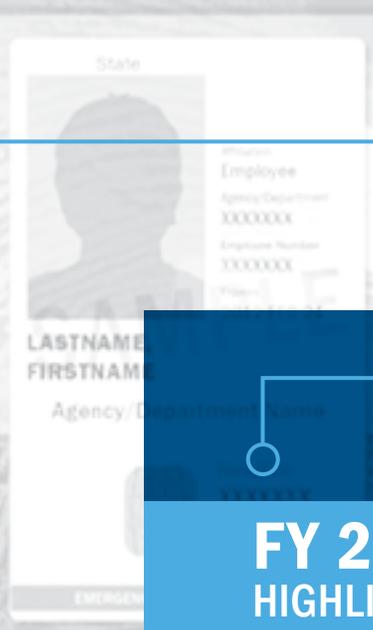
Credential Technology Transition Working Group (TTWG), which is primarily composed of federal, state, and local emergency management representatives. Through the TTWG, members

CSD is researching and developing identity management technologies to enable seamless and secure interactions among federal, state, local, and public-private sector stakeholders. S&T brings together these stakeholders on a quarterly basis through the Personal Identity Verification–Interoperable (PIV-I)/First Responder Authentication

share lessons learned; provide policymakers with a unified emergency manager perspective; and identify technology and capability gaps where CSD can provide research, development, testing and evaluation support. In 2007, S&T established the Identity Management (IdM) Testbed to explore and evaluate identity, credentialing, and access management architectures. S&T is leveraging the IdM Testbed to mitigate operational risks by developing proof-of-concept solutions, guiding standards development, conducting pilots, and demonstrating the utility of proposed solutions. This project is leading the way toward the use of technical standards in identity management architectures and credentialing interoperable, secure, cost-efficient solutions for managing identities and access control through the development of identity management tools.

The following benefits are provided by these identity management tools:

- Maintains the sovereignty between two organizations
- Eliminates the need for one organization to manage and maintain user identities of another organization. For example, if a DHS employee is visiting a military base, they will not be issued a visitor badge (less secure) or Department of Defense (DOD) Common Access Card (costly)
- Provides a technical and interoperable solutions for accepting cross-domain identification cards and user attributes, reducing the need for multiple credentials



FY 2013 HIGHLIGHTS

- Developed the Financial Institution – Verification of Identity Credential Service Gateway to improve identity proofing procedures and reduce the risk of identity fraud within the financial services sector. The gateway capability is under review by S&T and the White House for final transition to the Financial Services Sector Coordinating Council.
- Through the S&T Small Business Innovation Research (SBIR) program, successfully transitioned a capability for Physical Access Control Systems to interoperate with Logical Access Control Systems, demonstrating efficiency and enhancing physical security at government buildings in Washington, D.C.



PERFORMERS

- Johns Hopkins University, Applied Physics Laboratory
- PIVPointe
- Queralt Inc.
- Space and Naval Warfare Systems Center Atlantic
- SRI International



WEBSITE

<http://ahcusa.org/PIV-I%20TTWG.html>



PROGRAM MANAGER

Karyn.Higa-Smith@st.dhs.gov



CYBER CRIME



LAW ENFORCEMENT SUPPORT

As cyberattacks become more frequent, law enforcement agencies must be prepared to address the cyber threat landscape. Criminals are increasingly using the newest technologies and devices to commit crimes, forcing law enforcement to keep up despite budgetary restrictions. CSD provides the tools and techniques needed for investigating the use of computers and portable media devices (e.g., cell phones, GPS devices) in criminal and terrorist activities.

In FY 2013, CSD carried out the Law Enforcement Support program through one project.

CYBERSECURITY FORENSICS

Law enforcement officers and forensic analysts face the challenge of staying ahead of advances in computer and mobile device technology. CSD is developing new cyber forensic analysis tools and investigative techniques to aid in the analysis of information stored in constantly evolving hardware and software.



CYBERSECURITY FORENSICS

As ownership and use of electronic devices such as computers, mobile phones, and tablets increases, it is increasingly common to find such devices used during criminal activity. More often than not, digital evidence is involved in law enforcement investigations and may result in information central to criminal cases. Law enforcement agencies face a constant challenge of keeping pace with the latest technologies as technology's role has become more significant in criminal and terrorist investigations. Because new versions of devices and completely new technologies are quickly introduced to the consumer market, the methods for acquiring and analyzing digital evidence frequently change.

In response to this challenge, CSD initiated the Cybersecurity Forensics project in 2009 to support the specific needs of federal, state, and local law enforcement agencies. Through this project, CSD is developing new cyber forensic analysis tools and investigative techniques for law enforcement officers and forensic examiners to address the full range of crimes. Additionally, CSD sponsors the Cyber Forensics Working Group, which meets semiannually to discuss new requirements and ongoing work. Participation in the working group is open to all federal, state, and local law enforcement agencies.

During FY 2013, the project focused on portable media devices. One effort examined the problem of cheap, disposable cell phones ("burner" phones), which often do not have the external connections needed to acquire information. The

effort targeted 13 of the most popular phones and developed tutorials to guide law enforcement in unlocking the phones and collecting information from the device. Within the first two weeks of its availability, CSD and the performer viaForensics received more than 300 requests from law enforcement agencies for the tutorial documents.

Another challenge facing law enforcement investigators is the inability to create forensically sound images of NAND flash memory, which is commonly used in mobile device technology. Correctly extracting and verifying the information collected from these devices is challenging due to a number of issues including the routine overwriting of memory and noncontiguous manner data is stored in flash chips. A CSD effort successfully created a cell phone forensics tool for law enforcement investigators that addresses the problem of imaging the non-volatile rewritable memory chips found in phones. The tool provides law enforcement with a less invasive and less time-consuming method of conducting mobile phone forensics.

Additionally, CSD examined solid state drives (SSDs) and the unique challenges they present for forensic examiners. SSDs are increasingly found in consumer products such as laptops and traditional computer forensic approaches do not effectively translate to those investigations involving flash memory-based SSDs. At the end of FY 2013, CSD expanded research efforts to focus on providing hardware and software solutions.

FY 2013 HIGHLIGHTS

- Produced a set of unlock and analysis tutorials available for free to law enforcement through the Burner Phone Forensics effort. Additional information can be found at: <https://viaforensics.com/resources/tools/burner-phone-forensics/>
- Provided three-day GPS forensics training and one-year licenses to 80 participants from 36 federal, state, and local agencies.
- Published National Institute of Standards and Technology (NIST) Computer Forensics Tool Testing reports, which are publically available to the law enforcement community on the CyberFETCH website (<https://www.cyberfetch.org/>).



PERFORMERS

- Basis Technology
- Berla Corporation
- Exelis Inc.
- Naval Postgraduate School
- NIST
- S34A Inc.
- viaForensics



PROGRAM MANAGER

Megan.Mahle@hq.dhs.gov



NETWORK AND SYSTEMS SECURITY

Today's network systems security is built from the ground up and includes characteristics that are essential to the desired end states of trustworthy cyber systems. CSD is developing new and innovative approaches to mobile, Web, and cloud security that will enable the government and other users to take full advantage of the benefits that these technologies and services can offer. Furthermore, newly developed systems apply modeling and analysis capabilities to predict, understand, and respond to the effects of cyberattacks, including those by malicious insiders, on federal government and other critical infrastructure, with an emphasis on malware, botnets, situational understanding, and attack attribution.

In FY 2013, CSD carried out the Network and Systems Security program through seven projects.

MOBILE TECHNOLOGY SECURITY *(NEW START)*

The field of mobile device security has taken on greater importance with the influx of mobile technologies in the federal workspace. CSD created the Mobile Device Security project to address the need for mobile devices that can access greater capabilities without sacrificing the security necessary to maintain regulatory compliance and mission effectiveness.

INTERNET MEASUREMENT AND ATTACK MODELING (IMAM)

In order to better protect and defend the nation's critical Internet infrastructure and other assets, CSD must first identify which Internet resources are most vulnerable to attack and disruption. The IMAM project addresses this need by developing capabilities to map Internet hosts and routers. The project also conducts modeling and analysis to predict the effects of cyberattacks on commercial and federal infrastructure. The IMAM project is broken into three distinct focus areas: Network Mapping and Measurement, Modeling of Internet Attacks, and Resilient Systems and Networks.

SECURE CLOUD COMPUTING *(NEW START)*



Cloud computing is changing the way organizations deploy and manage information technology (IT) assets. However, the transition to the cloud is not without its risks, as the field introduces new vulnerabilities and methods of attack and compromise. To address these challenges, CSD's Secure Cloud Computing project seeks to develop technologies that can help organizations within the HSE better understand and mitigate the security implications of cloud computing.

MOVING TARGET DEFENSE (MTD)



The static and unchanging nature of our current IT systems provides the attacker with a huge advantage, allowing them to take their time and plan attacks at their leisure. To counter this threat, CSD funds the MTD project, which seeks to develop game changing capabilities that continually shift the attack surface, making it more difficult for attackers to strike. The MTD project also seeks to develop more resilient hardware that can continue to function while under attack.

TAILORED TRUSTWORTHY SPACES (TTS)



Cyberspace is composed of subsystems that cannot maintain or verify their security conditions with a high degree of confidence, which inhibits the establishment of a robust trust environment. To address this, CSD has established the TTS project, which aims to create distributed, consistently trusted environments that support functional, operational, and policy requirements.



ENTERPRISE LEVEL SECURITY METRICS

Meaningful metrics in cybersecurity have been difficult to develop because of the rapid evolution of IT as well as the continually shifting focus and methods of adversarial action. Through the Enterprise Level Security Metrics project, CSD seeks to develop security metrics and supporting tools and techniques to make them practical and useful as decision aids, allowing users and organizations to make informed decisions based on threats and costs.



INSIDER THREAT

Threats posed by untrustworthy individuals inside an organization are the source of numerous losses and have caused irreparable damage to national security interests. Through this project, CSD is developing a research portfolio to aggressively inhibit elements of this problem.



MOBILE TECHNOLOGY SECURITY (NEW START)

Mobile technology has greatly changed where and how people get work done. However, a lack of security is preventing some organizations from taking advantage of mobility. The lack of security is, in part, due to the economics of the mobile market, a market that is driven by consumers who are quick to adopt and are sold on features and capabilities; not surprisingly, phone developers have focused on that instead of enterprise security requirements. This has led to a model for mobile technology where the User has control over the device settings and its personalization. Additionally, the rise of mobile applications (or “Apps”) has also created the expectation of being able to easily add and remove an App as needed. This is at odds with the traditional approach to enterprise security, which is based upon being able to manage the end device and restrict its functionality and which applications it can load.

Within the Federal government, the potential impact of mobile technology is clear. Improving the government’s use of mobile technology is a cornerstone element in the 2012 Digital Government Strategy, led by the White House and the Federal CIO’s Council. A survey document, Government Use of Mobile Technology, was created as a follow up to the Digital Government Strategy, and it identifies how the government currently uses mobile technology, as well as barriers and opportunities to expanding its use. The report identified security and privacy as a major gap that needs to be addressed in order to enable more effective use of mobile technologies to meet government missions.

This project focuses on making mobile technology, like smart phones and tablets, more secure. This includes software to make them easier to manage, integration with PIV cards for user authentication, and solutions for evaluating the security of mobile apps. The result is that the government will be able to use mobile technologies without sacrificing security

This project began late in FY 2013 and specific research efforts and performers will be identified in FY 2014.



PROGRAM MANAGER

Vincent.Sritapan@hq.dhs.gov

9:57 PM

Enter Passcode

Passcode input area with four dots.

1

2

4

GHI

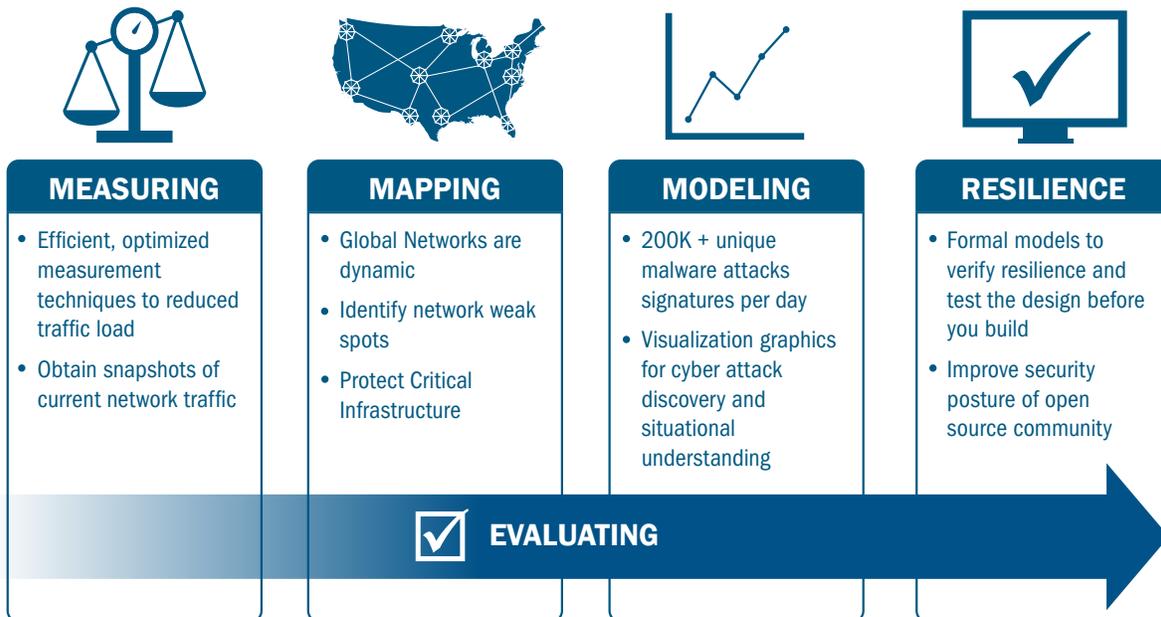




INTERNET MEASUREMENT AND ATTACK MODELING NETWORK MAPPING AND MEASUREMENT

The Internet is a vast and constantly changing phenomenon. It is important to understand the foundational elements of the Internet to optimize the user's experience, reduce the costs of measuring the Internet, and protect the nation's cyber infrastructure. IMAM's Network Mapping and Measurement performers scan the Internet and provide data about the current state, how outages affect user communities, and what can be done to improve network reliability. Performers also create data sets and provide them to the broader research community to study the Internet. Many knowledge products, in the form of academic papers, have also been produced.

In FY 2013, IMAM continued to provide robust data sets to government, commercial, and educational researchers, which can be used to map the Internet and detect weak spots or non-optimal routes. Additionally, IMAM worked to reduce the amount of probing necessary to gather this data in order to reduce total probe time and costs. Performers also explored ways to probe more accurately and minimize the disruption caused to those being probed.





FY 2013 HIGHLIGHTS

- Developed new adaptive techniques that enabled researchers to obtain the same amount of usable data as the current state-of-the-art techniques, but with a 60 percent reduction in the amount of disruptive probing.
- Funded improvements of Netalyzr, a network debugging tool that analyzes end-user connections and provides optimization recommendations. The Netalyzr tool added abilities for Domain Name System (DNS) queries, DNS Security Extension (DNSSEC), Border Gateway Protocol Security (BGPSEC), and Transport Layer Security (TLS). A mobile version of Netalyzr was also released as an Android application.
- Developed a new network measurement tool utilizing the Raspberry Pi computer. This tool has reduced the cost of setting up a network probing node from \$1000 per unit to just \$50 per unit.



PERFORMERS

- Merit Networks, Inc.
- Naval Postgraduate School
- University of California – Berkeley, International Computer Science Institute (USC - ICSI)
- University of California – San Diego, Cooperative Association for Internet Data Analysis (CAIDA)



WEBSITE

<http://www.caida.org/projects/cybersecurity/>



PROGRAM MANAGER

Ann.Cox@hq.dhs.gov



INTERNET MEASUREMENT AND ATTACK MODELING MODELING OF INTERNET ATTACKS

The growth in complexity of network systems has introduced new and larger attack surfaces for malicious actors to exploit. For example, an attacker can infiltrate one attack surface present in a network, such as the Voice over Internet Protocol (VoIP) phone systems that are present in most modern office environments, and use that foothold to gain access to other systems on the network that may have more sensitive information. Phones, printers, routers, and other networked devices are all subject to these kinds of non-trivial attacks. The Modeling of Internet Attacks focus area seeks to discover and model the diverse ways malicious actors can infiltrate systems and provide solutions for how to close the attack surface.

The multi-faceted approach of this area focuses on identifying, preventing, or mitigating an attack during three phases of the attack cycle: before an attack starts, as an attack is happening, and during the post-attack period. The CSD-funded software Symbiote is one technology solution that can identify an attack as it is happening and help speed recovery. Symbiote uses polymorphism and other software robustness techniques to secure the firmware of routers. By selecting and evaluating several vantage points from many that are randomly generated, Symbiote is able to detect every attempt to modify the firmware, send notifications, and enable implementation of mitigation techniques for the attack.



FY 2013 HIGHLIGHTS

- Completed a beta prototype of Symbiote, which is now being tested in the DHS-funded experimental research testbed known as DETER.



PERFORMERS

- Brigham Young University
- Columbia University
- Georgia Tech Research Corporation
- Oak Ridge National Laboratory
- University of Southern California, Information Sciences Institute
- University of Washington, Applied Physics Laboratory



PROGRAM MANAGER

Ann.Cox@hq.dhs.gov



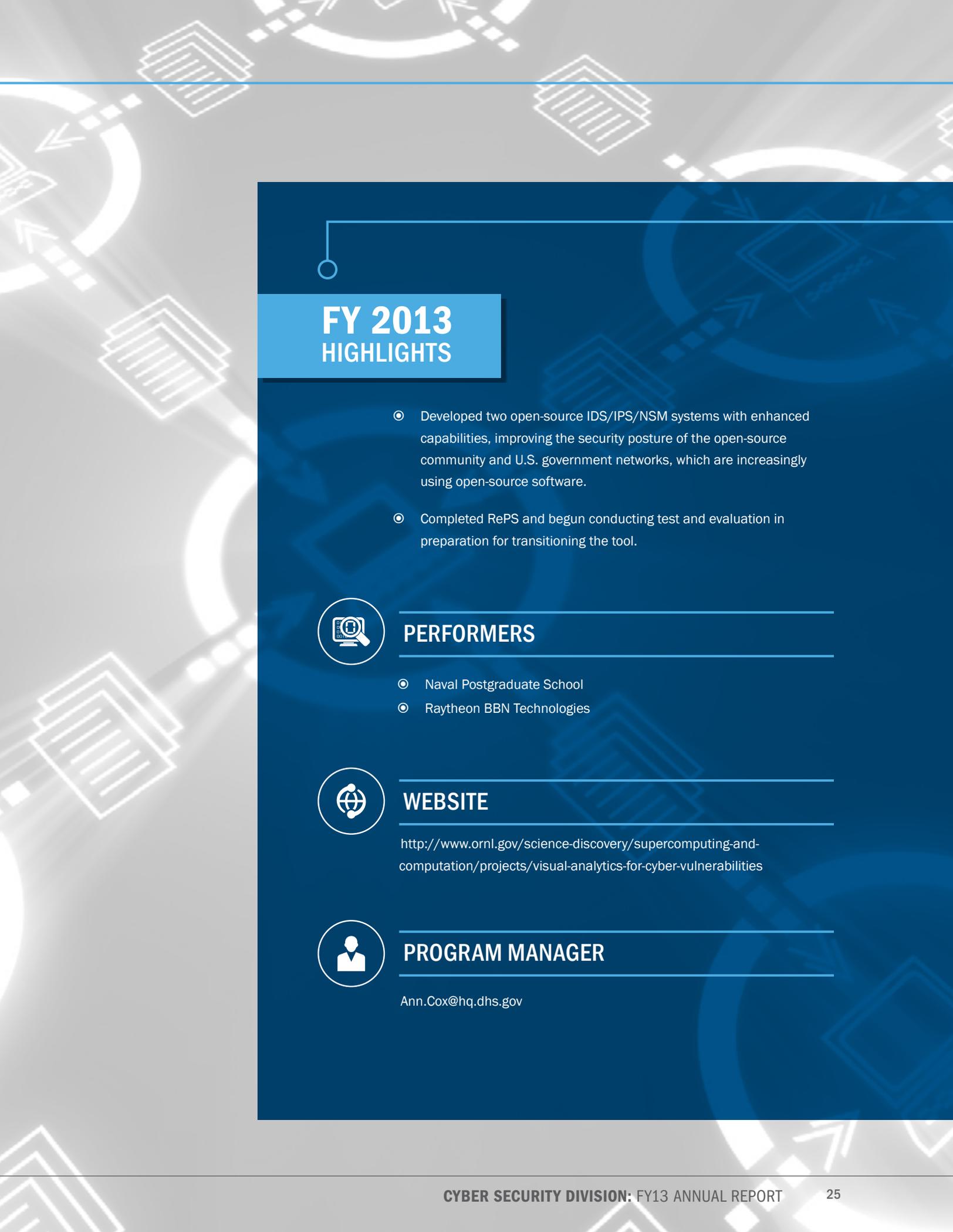
INTERNET MEASUREMENT AND ATTACK MODELING RESILIENT SYSTEMS AND NETWORKS

Often, detection and mitigation efforts are performed after an attack has already occurred. This occurs as a result of several factors, including malicious actors who constantly evolve their tactics, networks that are unable to detect threats and block them as they occur, and networks that are not designed to be secure from their inception. The Resilient Systems and Networks area of the IMAM project focuses on developing technologies to combat these problems.

One such technology is the Real-time Protocol Shepherds (RePS), which builds off of previous investments by the Defense Advanced Research Projects Agency (DARPA) in the field of Scalable

Network Monitoring (SNM). SNM capabilities can be incorporated into Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Network Security Monitoring (NSM), such as real-time protocol analysis that can identify and alert when network-based attacks are occurring. CSD has incorporated DARPA's previous work in SNM into the CSD-funded Suricata and Bro tools, which are open-source IDS/IPS/NSM products. With this advancement, an IDS/IPS/NSM is able to detect some zero-day attacks and even automatically create malware signatures as they are discovered rather than waiting days, weeks, or months for a human analyst to develop a signature.





FY 2013 HIGHLIGHTS

- Developed two open-source IDS/IPS/NSM systems with enhanced capabilities, improving the security posture of the open-source community and U.S. government networks, which are increasingly using open-source software.
- Completed RePS and begun conducting test and evaluation in preparation for transitioning the tool.



PERFORMERS

- Naval Postgraduate School
- Raytheon BBN Technologies



WEBSITE

<http://www.ornl.gov/science-discovery/supercomputing-and-computation/projects/visual-analytics-for-cyber-vulnerabilities>



PROGRAM MANAGER

Ann.Cox@hq.dhs.gov



SECURE CLOUD COMPUTING (NEW START)

Cloud computing is rapidly transforming IT in both the private and public sector. Cloud-based solutions provide significant scalability, realize significant cost effectiveness, can be quickly deployed and provisioned, and enable full transparency in managing operational costs. Because of these capabilities, organizations face enormous pressure to incorporate cloud solutions into their operational environment. However, the novel combination of technologies used to implement cloud services introduces new vulnerabilities to malicious attack, which will only increase as more applications move to the cloud. Enterprises that are concerned about the risks of migrating their systems to the cloud are unable to evaluate those risks because the underlying cloud infrastructure's vulnerabilities are owned by another organization and are hidden from them. Current cloud computing security approaches are based on virtualization, separation, and access control. However, compromised computing nodes must be manually identified and disinfected; they cannot be recovered quickly in the face of automated and persistent attack.

To address these gaps and more, in FY 2013 CSD began funding efforts in Secure Cloud Computing. One of these efforts is Cloud-COP, a revolutionary framework for a secure, mission-oriented, resilient cloud. Cloud-COP includes self-healing software mechanisms and, with the assistance of hardware, can regenerate compromised or faulty computing nodes from a pristine state stored in ROM. Task supervision and end-user communications are performed by the

Control Operations Plane (COP), which builds a trustworthy, resilient, self-healing, provably secure cloud out of the underlying untrustworthy and potentially faulty hosts.

CSD is also funding the development of Silverline, an expert tool for automatically detecting, evaluating, and mitigating cloud-specific security risks in cloud services. Silverline accomplishes this through several innovations: the ability to investigate applications that have already been deployed onto a cloud platform, the extension of the NIST Security Content Automation Protocol descriptions and automated testing tools to the cloud environment, the use of attack decision trees to relate possible modes of attack, and the creation of an underlying knowledge base including both vendor-supplied information and information gained through investigation.

FY 2013 HIGHLIGHTS

The Secure Cloud Computing project began in late FY 2013. In FY 2014, CSD plans to deliver the following technologies, demonstrations, or knowledge products:

- Simple and Generic Silverline attack trees
- Initial Silverline software demonstration
- Cryptographic protocols and algorithm performance assessment/design document
- Cloud-COP architecture design



PERFORMERS

- ATC-NY
- HRL Laboratories LLC



PROGRAM MANAGER

Edward.Rhyne@hq.dhs.gov



MOVING TARGET DEFENSE

Our IT systems are built to operate in a relatively static configuration on hardware that is presumed to be safe and trusted. This approach is the legacy of a time when malicious exploitation of system vulnerabilities was not a concern, so IT system design focused on functionality and simplicity. However, static systems present a substantial advantage to attackers. Attackers can observe the operation of key IT systems over long periods of time and plan attacks at their leisure. Despite the rapid technological growth over the past three decades of computing, today's hardware still only provides limited support for security, and capabilities that do exist are often not fully utilized by software. Therefore, there must be a game-changing approach to building capabilities. Hardware must be designed to continually shift the attack surface and to exhibit greater functional resilience while under attack.

To address these challenges, CSD is developing numerous MTD capabilities. Through the use of dynamic networks, platforms, hardware, and data, MTD takes the advantage away from the attacker by eliminating the static nature of modern systems. MTD strategies can employ architectures where one or more system attributes are automatically changed in a way that makes the system's attack surface appear unpredictable while still remaining functional to a legitimate user. These strategies can also be incorporated into hardware design to reduce the trusted computing base and attack surface, thus thwarting hardware-dependent vulnerabilities such as cache side-channel attacks.

One effort in the MTD project seeks to design a secure hardware cache that does not leak sensitive information through cache-based, side-channel attacks, as there are currently no reliable defenses against this form of attack. CSD plans to develop a Newcache hardware solution that is software- and performance transparent and can be integrated into existing software and hardware ecosystems.

CSD is also funding the development of Hardware Enabled Zero-Day Protection (HEZDP)—a comprehensive security solution utilizing Unified Extensible Firmware Interface (UEFI) for user space protection. HEZDP uses a full spectrum approach across multiple layers with hardware being the cornerstone for thwarting attacks. The HEZDP software starts at the firmware level and is applied in the operating system kernel to provide comprehensive resilience against all forms of malicious activity.

The magnitude of the problem arising from the current state of our static systems and networks requires a varied and thorough approach across many technical areas. The diversity of the proposed solutions illustrates the depth of the challenge. In addition to the technical challenges, it requires a shift in mindset away from the way networks have typically been structured.



FY 2013 HIGHLIGHTS

- Completed the initial Appliance for Active Repositioning in Cyberspace effort and began planning steps toward deployment and commercialization.
- Submitted the Newcache test-chip to a foundry for prototype production.
- Designed prototype for a secure mobile environment and endpoint.
- Developed the HEZDP master test plan and system design/functional specifications.



PERFORMERS

- Def-Logix Inc.
- Endeavor Systems
- IBM Thomas J. Watson Research Center
- Northrop Grumman Information Systems
- Princeton University



PROGRAM MANAGER

Edward.Rhyne@hq.dhs.gov



TAILORED TRUSTWORTHY SPACES

Cyberspace—and the computer networks and critical cyber infrastructure that it comprises—cannot establish and maintain secure conditions with a consistent, high degree of confidence. Consequently, the security of environments used for exchanging data, stored information or applications needs to be verified constantly. CSD's TTS project comprises five separate efforts that investigate different approaches toward ensuring the *trustworthiness* of networks, rather than their security. These five efforts are grouped into two complementary areas: Digital Provenance and Nature-inspired Cyber Health—technical topic areas that were called out for research in the 2011 White House-led Trustworthy Cyberspace Strategic Plan for the Federal Cybersecurity Research and Development Program.

Consider provenance first. The term signifies the authenticity or source of an object or, as in the cyber realm, a digital object. Provenance means that the object has not been altered or manipulated and that the user or recipient of the data or code is certain about its origin and previous users; in other words, the user knows whether or not the data or code can be “trusted.” The three efforts being funded in the area of Digital Provenance address:

- *Evidentiary integrity* – a response tool for cyber incidents that ensures evidence collection and management are controlled and that a chain of custody (analogous to that used for crime scene evidence) can be established for digital data associated with a cyber-attack.

- *Controlled access to medical records* – a method for tracking, logging, and blocking access by authorized or unauthorized persons to digital information on disks, in memory, or across a network
- *Auditing of cell phone locations* – an application that protects the integrity and confidentiality – and preserves the privacy - of location data collected by mobile devices

The two efforts in the Nature-Inspired Cyber Health area are more complex. They both attempt to use protective behaviors adopted by biological systems as analogues for more quickly detecting anomalous (or “unknown”) software code or network intrusions quicker than current technique. Furthermore both efforts rely on distributed decision-making rather than identifying and detecting specific threat signatures at specific nodes. The draft Cybersecurity Framework being developed by the National Institute of Standards and Technology (NIST) in response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity, has specifically identified “detection” of anomalous code or network behavior as one of the five essential approaches to mitigating cyber threats. The two efforts being funded in the area of Nature-inspired Cyber Health address:

- *LINEBACKER* – a system for identifying patterns and trends in network traffic - based on translating packets, groups of packets, and even netflows into sequences or clusters of letters in real time.

- ◎ *BIAD* – a new model to detect potential cyber-attacks, which mimics the communication and decision-making techniques adopted by social insects to alert them of possible dangers. Additionally this effort is an architecture testbed comprised of tens of thousands of routers and switches capable of demonstrating how DDOS attacks, botnets, or worms affect network operations.



FY 2013 HIGHLIGHTS

- ◎ Demonstrated evidence integrity prototype to three law enforcement agencies in New York and established agreements to begin piloting the beta version of the prototype by the end of 2014.
- ◎ Demonstrated a capability to track the chain of custody for digital records and log any and all accesses to those records across a network. The system will be piloted at the Carolina Data Warehouse for Health as part of North Carolina's Secure Medical Research Workspace project.
- ◎ Successfully demonstrated a smartphone application and location proof server as part of a secure location provenance effort.
- ◎ Demonstrated 20-40 percent improvement of detection of anomalous code. Code sequences are being shared with the Department of Energy's computer network.



PERFORMERS

- ◎ Exelis Inc.
- ◎ Rutgers University
- ◎ Pacific Northwest National Laboratory
- ◎ University of Alabama at Birmingham
- ◎ University of North Carolina at Chapel Hill



PROGRAM MANAGER

Joseph.Kielman@hq.dhs.gov



ENTERPRISE LEVEL SECURITY METRICS

Metrics quantify progress in many system security areas, such as physical security, but are lacking in other areas such as information security. Defining information security metrics has proven challenging because the general community cannot come to consensus on which types of metrics are useful and what should be measured. This is due in part to the rapid evolution of IT, as well as the shifting focus of adversarial action. However, these metrics are greatly needed; without sound and practical information security metrics, progress in both researching and engineering secure systems is severely hampered.

To address this need, CSD started the Enterprise Level Security Metrics project to help organizations address the security posture of their IT infrastructure. These metrics address the

question of whether an organization's security mechanisms are enough to defend against or respond to security threats. Experts, such as system administrators, and non-technical users alike must be able to use an organization's system while maintaining security. To ensure this level of usability, CSD is developing security metrics and supporting tools and techniques to make the metrics practical and useful decision aids. This project will enable users to measure security while achieving usability and to make informed decisions based on threats to the organization. Additionally, owners and operators will be able to analyze security metrics over a period of time and understand the impact of adding or removing specific systems and security policies.







FY 2013 HIGHLIGHTS

- Produced a tool for measuring enterprise network security risk that can be integrated into the Cauldron attack graphing tool. This tool leverages data sources that are commonly deployed within enterprise networks, such as vulnerability scanners and firewall configuration files.
- Developed a metrics tool to integrate into the NP-View technology developed by the University of Illinois, Urbana-Champaign. The metrics tool will provide a snapshot of an organization's current security levels, allowing users to pinpoint where the most important security vulnerabilities exist. This information will assist users in preparing for security audits. Network Perception, a commercial company created for this technology, will continue to test the metrics through pilots and offer it in a commercial package with other security technologies.



PERFORMERS

- University of Illinois, Urbana-Champaign
- George Mason University



WEBSITE

Network-perception.com



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



INSIDER THREAT

Cybersecurity measures are frequently focused on threats from outside an organization rather than threats posed by untrustworthy individuals inside an organization. However, insider threats are the source of many losses, such as financial, intellectual property, personal information in critical infrastructure industries. Additionally, well-publicized insiders have caused irreparable harm to national security interests. ***An insider threat can be defined as the potential violation of system security policy by an authorized user.*** Although policy violations can be the result of carelessness or an accident, the main concern is deliberate and intended actions. Examples of such insider actions are malicious exploitation, theft, or destruction of data, or the compromise of networks, communications, or other IT resources. The CSD Insider Threat project is developing a research portfolio to aggressively curtail elements of this problem.

One effort involves developing a new approach for detecting hostile insiders by looking for individuals whose storage behavior diverges from their prior behavior and that of their peers. A lightweight forensics software agent is run on each computer workstation within an organization and is then able to identify workstations with unusual statistical properties that warrant further analysis. The proposed solution will provide organizations with an ability to detect hostile insiders—specifically insiders who are collecting information on their computers either for personal use inconsistent with organizational norms or with the intent of later exfiltration.

Another FY 2013 effort focused on researching, developing, deploying, evaluating, and demonstrating data exfiltration detection techniques in realistic controlled and operational environments. Through this effort, CSD aims to ensure the applicability and transferability of funded research to the commercial marketplace. While data exists throughout an organization, the exfiltration of data residing in an organizational database management system (DBMS) may pose one of the greatest threats to security. By studying the patterns of interaction between users and a DBMS, it is possible to detect anomalous activity that is indicative of early signs of exfiltration. An anomaly and misuse detection system, such as the one being developed through this effort, that operates at the data source prevents data from leaving the source before it escapes into an organizational network where it is hard to track.

The solutions developed through this project will benefit a wide range of customers, including national security bodies; government officials who need to share sensitive-but-unclassified or controlled unclassified information; and healthcare, finance, and other critical infrastructure sectors where sensitive and valuable information is managed.



FY 2013 HIGHLIGHTS

- CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute completed their effort briefing the "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector" to US Secret Service-sponsored Electronic Crimes Task Forces



PERFORMERS

- Carnegie Mellon University
- Naval Postgraduate School
- Northrop Grumman



PROGRAM MANAGER

Megan.Mahle@hq.dhs.gov



RESEARCH INFRASTRUCTURE

Cybersecurity research and development involves understanding new threats and risks and discovering solutions that will protect our nation's cyber infrastructure. The Research Infrastructure program provides a national- and international-level research infrastructure that enables the cybersecurity research community to discover, test, and analyze state-of-the-art tools, technologies, and software in a scientifically rigorous and ethical manner. By having a research infrastructure that mimics real-life conditions, this program accelerates the research, development, and deployment of effective defenses for computer networks and systems.

In FY 2013, CSD carried out the Research Infrastructure program through three projects.

○ **EXPERIMENTAL RESEARCH TESTBED (DETER)**

The Experimental Research Testbed, also known as the DETER testbed, enables cybersecurity researchers to run experiments on a “virtual Internet.” This allows researchers to safely test advanced defense mechanisms against “live” threats without endangering the larger Internet.

○ **RESEARCH DATA REPOSITORY (PREDICT)**

In order to support the cybersecurity research community in its mission to accelerate the design, production, and evaluation of next generation cybersecurity solutions, CSD has created and maintains the Research Data Repository, also known as PREDICT. This repository provides researchers with large scale data sets containing real network and system traffic, allowing researchers to expose their solutions to realistic traffic and operating conditions.



EXPERIMENTAL RESEARCH TESTBED

It is important that new cybersecurity approaches get evaluated in a realistic environment. The Experimental Research Testbed project, also known as the DETER testbed, can create a “virtual Internet” that is scalable and secure. The testbed’s self-contained environments allow researchers to safely test advanced defense mechanisms against “live” threats without endangering other research or the larger Internet. The DETER testbed is currently used to test and evaluate cybersecurity technologies by more than 200 organizations from more than 20 states and 30 countries, including major DHS-funded researchers, government, industry, academia, and educational users.

The DETER testbed provides the necessary infrastructure—networks, tools, methodologies,

and supporting processes—to support national testing of emerging and advanced security technologies. CSD’s current efforts to further develop the testbed will support larger and more complex experiments with increased usability.

The success of the DETER testbed can be attributed to close collaboration with the cybersecurity research community. Annual workshops are conducted to disseminate and discuss project results and outcomes, and CSD has published reports documenting benchmarks, testbeds, data collection and analysis, and evaluations of security mechanisms that have been deployed.





FY 2013 HIGHLIGHTS

- Released automation tools for DETER that make repeatable experiments much easier. These tools were used by both the DARPA Safer Warfighter Communications (SAFER) user group and the GridStat community. This release provides new group communication models, agent reliability, monitoring and acquisition, and toolkits.
- Released DETER code 0.93, which includes features to make standing up a new DETER node easier.
- Initiated an effort to develop a unified application programming interface (API) highlighting the unique DETER-specific capabilities to allow for a powerful, principled, and integrated system. A complete specification of the API has been developed along with initial implementation, regressions tests, and a preliminary DETER beginner's interface.



PERFORMERS

- University of Southern California, Information Sciences Institute



WEBSITE

<http://deter-project.org/>



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



RESEARCH DATA REPOSITORY

The Research Data Repository, also known as PREDICT, is the only freely available, legally collected repository of large-scale data sets containing real network and system traffic. PREDICT provides technology developers and evaluators a variety of real-world data sources and types to determine the efficacy of their technical solutions. The distributed repository has three key components: data providers, data hosts, and a coordinating center that provides a centralized mechanism for cataloging available data while managing the submission and review of data requests. PREDICT's distributed structure provides secure, centralized access to multiple sources of data and promotes data sharing.

In FY 2013, the cybersecurity research community increasingly used PREDICT to support their research, including international partners in Japan, Canada, Australia, and Israel. CSD began researching ways to better automate the legal framework for the purpose of providing quicker access to data sets. The Web portal (<https://www.predict.org>) was significantly modified to incorporate different data categories, each with a different process, in an effort to streamline access to data sets with fewer restrictions. These changes laid the groundwork for including a wider variety of data sets in the repository. CSD also began implementing virtual data enclaves to provide remote access to select data sets in an audited environment.

Other related activities include: continuing to promote a better understanding of the ethical implications of cybersecurity research that resulted in publishing responses to comments received about the *Menlo Report* in the Federal Register and an inaugural Cyber-security Research Ethics Dialogue & Strategy (CREDS) Workshop sponsored in conjunction with the IEEE Symposium on Security and Privacy.



FY 2013 HIGHLIGHTS

- Added new customers and partners to the project, including 17 academic institutions, 21 commercial organizations, 3 foreign partners, 8 government agencies, and 2 non-profit organizations.
- Added 105 new data sets.
- Approved 139 new accounts.



PERFORMERS

- Georgia Tech Research Corporation
- Global Cyber Risk LLC
- Packet Clearing House
- Research Triangle Institute International
- University of California, San Diego
- University of Michigan
- University of Southern California, Information Sciences Institute
- University of Wisconsin



WEBSITE

<https://www.predict.org>



PROGRAM MANAGER

Douglas.Maughan@hq.dhs.gov



SOCIAL-BEHAVIORAL EDUCATION, LEARNING, AND TRAINING

The Social-Behavioral Educational, Learning, and Training program improves the human element of cybersecurity through multi-disciplinary research into technology usability, workforce development, education, team and multi-team training, incentives, and behavioral analysis.

In FY 2013, CSD carried out the Social-Behavioral Educational, Learning, and Training program through four projects.

USABLE CYBERSECURITY

To help IT owners and operators balance the tradeoffs between security and functionality, the Usable Cybersecurity project seeks to develop security solutions that are intuitive and easy for users to understand, thus improving the likelihood that they will be correctly and effectively implemented.

CYBER ECONOMIC INCENTIVES

CSD is studying the economic factors, conditions, and incentive structures for security measures to help organizations better understand the value of implementing cybersecurity measures into business operations and to encourage stakeholders to behave in a manner that will improve overall security.

CYBERSECURITY COMPETITIONS

Ensuring that the nation has a highly skilled cybersecurity workforce is of the utmost importance to maintaining the continued functioning of our nation's systems and networks. The Cybersecurity Competitions project aims to overcome the shortage of technically skilled people required to operate and support deployed systems by exposing high school and college students to robust cyber competition challenges.

INCIDENT RESPONSE COMMUNITIES

Cybersecurity Incident Response Teams (CSIRTs) are vital to responding to network events and mitigating damage and consequences. The Incident Response Communities project is studying effective CSIRTs to determine the methods and characteristics that go into making an effective response team.



USABLE CYBERSECURITY

The importance of cybersecurity has never been more important, yet implementing strong security can be difficult for both the common user and the trained professional. Implementing and operating a secure system on home PCs, mobile phones, and tablets is often not the first priority for home users, and IT owners and operators must balance the tradeoffs between security and functionality. There is a need for security solutions that are more intuitive and easy for users to understand. In addition, security at the enterprise level should have a minimal footprint on the user and operate in the background, without user interaction.

CSD is conducting research into the usability of security solutions through three efforts. The goal of these efforts is to understand how users interact with their systems and how they interpret and react to security issues that are presented to them. One effort is focused on how people

react when presented with different contextual risks, leading to a better understanding of how users balance security concerns and functionality. CSD is also researching how to leverage sensors in mobile phones and tablets to authenticate users. In addition, CSD is developing technologies that can determine risk levels and adjust authentication requirements based on the value of the transaction and the apparent risk.

These technologies will allow both individuals and enterprise IT operators to more easily use security solutions. The burden of using security tools will no longer impact how users interact with their IT systems. The studies will also lead to new technologies that make it easier to understand the risks when making specific IT decisions. Combined, these technologies will create a more secure user interface that will have a negligible impact on users' functionality.



FY 2013 HIGHLIGHTS

- Implemented touch-based gesture authentication module on Android and iPhone devices, enabling continuous identity verification in the background. Published research results in the IEEE International Conference on Biometrics: Theory, Applications and Systems 2013, IEEE International Symposium on Trust and Identity in Mobile Internet, Computing and Communications 2013, IEEE International Conference on Technologies for Homeland Security 2013, and HotMobile 2014.
- Organized a Risk in IT workshop in conjunction with the Symposium on Usable Privacy and Security.
- Completed the initial implementation of new communication frameworks, including a novel out-of-band authentication framework that allows applications to support new authentication modalities without modification, greatly improved security and privacy.



PERFORMERS

- IBM
- Indiana University
- University of Houston



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



CYBER ECONOMIC INCENTIVES

Despite the growing focus on and widespread interest in cybersecurity, at least one aspect of this multi-dimensional problem has received relatively little attention from the research community—the economic, behavioral, or business factors that induce the private sector to select and implement cybersecurity measures. For example, little data has been collected or validated regarding how much is being spent on cybersecurity in the private sector, let alone the government sector. Likewise, the amount of damage—immediate and long term—caused by various cyberattacks or threats has not been accurately measured.

Furthermore, there is a lack of tested models to determine the ultimate value of cybersecurity measures, as well as data on business-oriented measures such as return on investment or competitive advantage obtained from adopting cybersecurity.

The federal government can use various techniques to broaden the appeal and implementation of cybersecurity measures by the private sector. These incentives include regulatory, policy, legal, insurance, or financial means. Determining how effective incentives are in helping private firms, critical infrastructure operators, and industry organizations better secure their networks and data is one of several objectives of CSD's research efforts.

A complementary interest for government is identifying disincentives that will discourage

criminal or terrorist organizations from engaging in cybercrime or cyberattacks. It is important for law enforcement agencies and security staff at private sector firms to anticipate criminal or terrorist behaviors and to identify specific internet nodes they are likely to use for their attacks. Such information can make it more difficult or too expensive and resource-intensive for criminal gangs or terrorist groups to operate. This research will also help law enforcement agencies ensure the integrity of evidence collected through investigations of cybercrime.

The three efforts in CSD's Cyber Economic Incentives project ultimately address business decision-making questions such as:

- Where and how much should the private sector invest in cybersecurity?
- How can law enforcement alter the behaviors and motives of criminal enterprises investing in cybercrime?
- In the absence of incentives, how effective are cybersecurity measures adopted through the self-regulating or self-motivated actions of firms or organizations?

The impact of this work will be realized through the production and use of:

- Actual data on the relative value of cybersecurity measures.
- Testable models or mathematical rules for determining where, how much, and on what measures to invest.

- ⦿ Models for cybercriminal activities and Internet supply chains applicable to financial crimes and Internet trafficking of drugs and humans.
- ⦿ Affordable and usable information-sharing schemes and networks that enable law enforcement agencies or private organizations to coordinate and prevent crimes or minimize threats.

Unlike other research efforts, the methods being investigated focus on business aspects rather than technical aspects. By measuring the market or business value of cybersecurity targeted, lower-cost investments can be made that both control the effects of cyber threats and mitigate the risks of cybercrime and cyberattacks.

FY 2013 HIGHLIGHTS

- ⦿ Developed an analytical technique for business investments that extends the University of Maryland's widely accepted model for implicit (or internal) cost to cover externalities, such as the total social and infrastructure costs.
- ⦿ Developed and tested survey instruments for five case studies.
- ⦿ Developed large-scale industry surveys to collect actual data on cybersecurity expenditures and damages from cyberattacks.
- ⦿ Identified cybercrime indicators and developed models of criminal cyber supply chains for online pharmacies, including the domain chokepoints (or nodes used for managing illegal transactions).
- ⦿ Developed formats and standards for exchanging cybercrime data across government, law enforcement, industry, and academia.



PERFORMERS

- ⦿ Carnegie Mellon University
- ⦿ University of Maryland
- ⦿ University of Michigan



PROGRAM MANAGER

Joseph.Kielman@hq.dhs.gov



CYBERSECURITY COMPETITIONS

Developing cutting-edge cyber defense technologies and capabilities is critical to maintaining the nation's advantage in cyberspace. However, they are useless if there are no qualified, skilled people in the workforce to operate them. In an effort to address the pressing need for a well-trained cyber defense workforce for the future, CSD has assisted with the development of cybersecurity competitions. The Cybersecurity Competitions project helps fulfill the challenge presented in Priority III of the National Strategy to Secure Cyberspace to “foster adequate training and education programs to support the Nation's cybersecurity needs.” Cybersecurity competitions are designed to help overcome the shortage of technically skilled people required to operate and support systems already deployed. They also educate and prepare students to design secure systems and create sophisticated tools needed to prevent malicious acts.

In FY 2013, CSD continued to provide funding to support the development and execution of the National Collegiate Cyber Defense Competition

(NCCDC). More than 1,920 students from 160 colleges and universities participated in NCCDC events, which included 14 qualifying rounds, 10 regional events, and one national championship. In the 2013 NCCDC season, competition organizers worked with CSD to integrate other CSD-supported efforts and technologies, such as Personal Identity Verification Interoperability, or PIV-I, cards and multiple network visualization tools, into NCCDC events. Integrating these research projects provides CSD with additional piloting opportunities for the technologies and exposes students to advanced technologies and research efforts.

Funding from CSD also helped support the development of training materials for teams participating in CyberPatriot, the nation's largest high-school-level cyber defense competition with more than 1,200 teams of two to five students participating. In addition, CSD supported the U.S. Cyber Challenge (USCC), which conducts competitions and cyber summer camps. In FY 2013, nearly 1,500 students participated in the USCC Cyber Quest competitions to qualify for one of the summer cyber camps. USCC conducted four cyber camps with more than 200 students during the summer of 2013. Each camp featured four days of intense instruction and culminated in a cyber “Capture the Flag” competition. USCC also conducted multiple rounds of CyberFoundations competitions—entry-level high school competitions focused on the fundamentals of cybersecurity, including networking, operating systems, and system administration.





FY 2013 HIGHLIGHTS

- Continued development of the CyberCompEx virtual community:
<http://www.cybercompex.org>
- Conducted a cybersecurity competition at the Australian Security in Government Conference.
- Supported cybersecurity competitions with more than 7,000 students.



PERFORMERS

- Council on CyberSecurity
- University of Texas at San Antonio, Center for Infrastructure Assurance and Security



WEBSITE

<http://www.nationalccdc.org/>
<http://www.uscyberchallenge.org>



PROGRAM MANAGER

Edward.Rhyne@hq.dhs.gov



INCIDENT RESPONSE COMMUNITIES

The characteristics of individuals, teams, and communities that contribute to an outstanding CSIRT have not been studied and documented to the level of detail in other areas where this is essential, such as with first responders, commercial pilots, and military personnel.

By analyzing documentation, observing CSIRT activity, convening focus groups, using pre- and post-incident interviews, and applying scenarios, a team from Dartmouth College, George Mason University and Hewlett-Packard are developing recommendations to improve the skills, dynamics, and effectiveness of CSIRTs. This research will determine and validate the principles of

creating, running, and sustaining an effective CSIRT. The output will include descriptions of needed knowledge, skills, and abilities for key CSIRT roles viewed from individual, team, and multi-team system perspectives. Through this project, CSD will also produce simulation-derived recommendations for optimal CSIRT performance that take into account available resources and organizational and national risk. Ultimately, this project will result in a set of guidelines for CSIRT creation and management, as well as a set of decision aids for optimizing effectiveness and encouraging CSIRT members to follow demonstrably effective practices and products.





FY 2013 HIGHLIGHTS

- Developed a taxonomy of CSIRT performance dimensions at the individual, team, and multi-team level and validated against the National Initiative for Cybersecurity Education.
- Collected and analyzed preliminary data from focus groups on CSIRT triggers, or what causes a CSIRT to respond to an incident.
- Completed preliminary documentation of CSIRT processes through interviews with CSIRT teams from a range of companies.



PERFORMERS

- Dartmouth College
- George Mason University
- Hewlett-Packard Company



PROGRAM MANAGER

Scott.Tousley@hq.dhs.gov



SOFTWARE ASSURANCE

The nation's critical infrastructure (energy, transportation, telecommunications, banking and finance, and more), businesses, and services are extensively and increasingly controlled and enabled by software. However, vulnerabilities in that software put those resources at risk. This risk is compounded by the size and complexity of software, the ways in which software is developed and maintained, the use of software produced by non-vetted suppliers, and the interdependence of software systems. The Software Assurance program develops fundamental technologies and approaches for ensuring that critical software is free from weaknesses that lead to vulnerabilities that could be exploited by adversaries.

In FY 2013, CSD carried out the Software Assurance program through two projects.

○ **SOFTWARE QUALITY ASSURANCE (SQA)**

The SQA project seeks to develop tools and technologies that can improve the quality and reliability of software, as well as improve how software systems are designed, developed, and maintained.

○ **SOFTWARE ASSURANCE MARKETPLACE (SWAMP)**

SWAMP provides a national level resource in software assurance for open security technologies used in civilian agencies and their communities. SWAMP is used as a research platform and is instrumental in the development and transition of U.S. government software



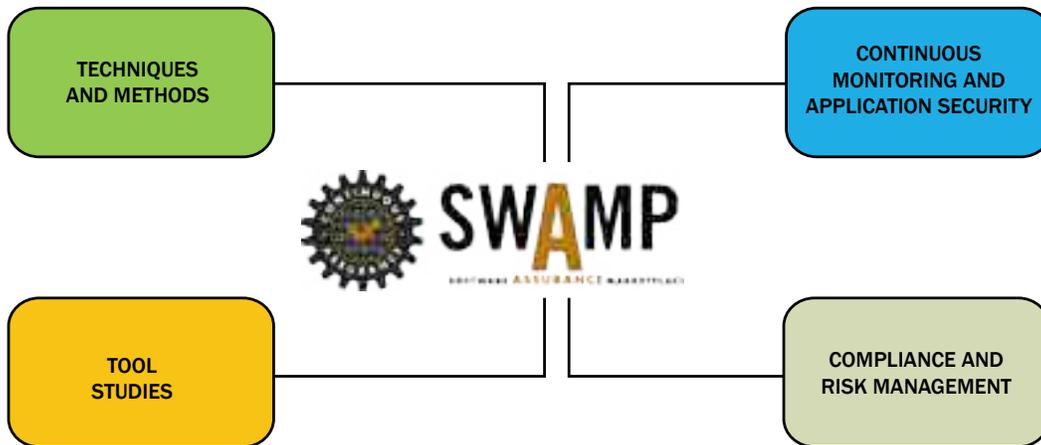
SOFTWARE QUALITY ASSURANCE

The overall cost of fixing or removing software bugs has been on the rise since a study conducted by NIST in 2002 suggested software failures cost the U.S. economy \$59.5 billion annually. A more recent study conducted by University of Cambridge in 2013 suggests that software bugs cost the global economy \$312 billion annually. Software assurance tools have not kept pace with the evolution of software, which has grown increasingly complex and large. This presents unique challenges in the performance of software evaluation tools, such as how well tools perform in the areas of precision, soundness, and scalability. These characteristics help users better understand the breadth and depth of software quality assurance tools in keeping pace with software in terms of complexity and size.

The SQA project creates breakthroughs and advancements in techniques, methods, and services for software analysis tools and testing. The goal of the SQA project is to create better

performing tools that can be adopted earlier in the Software Development Life Cycle (SDLC) to assist developers in finding and identifying software bugs, defects, and weaknesses before software leaves their desktop. Studies have shown the cost to fix a software bug, defect, or weakness significantly increases as it moves through each phase of the SDLC.

In FY 2013, the SQA project initiated several efforts to provide innovative and improved SQA tools and technologies. These new efforts are aligned with CSD's Software Assurance key program areas—**Tool Studies, Techniques and Methods, Continuous Monitoring and Application Security, and Compliance and Risk Management.** The SQA tools and techniques developed in this program will be integrated into SWAMP, which is designed to provide a collaborative research environment where software developers and researchers can exchange ideas, test their software, and improve their tools.



FY 2013 HIGHLIGHTS

- Successfully completed Phase I of the Hybrid Analysis Mapping SBIR project.
- Bundled open-source tools, including FindBugs, PMD, JSHint, and Cppcheck, as part of the Code Dx technology. Code Dx was developed as part of an effort that is designed to normalize and correlate outputs from disparate static analysis tools.
- Transitioned key research technology developed under the SQA project to GrammaTech's commercial flagship technology, CodeSonar.



PERFORMERS

- Applied Visions
- HRL Laboratories LLC
- Kestrel Technology
- Secure Decisions
- University of Nebraska



WEBSITE

<https://continuousassurance.org/tool-selection/>



PROGRAM MANAGER

Kevin.Greene@hq.dhs.gov



SOFTWARE ASSURANCE MARKETPLACE

Software has become an essential component of our nation's critical infrastructure. It has grown in size, capability, and complexity at a rate that exceeds our ability to keep pace with ensuring its quality. Through continuous assurance services, SWAMP helps narrow the gap that exists in the way software is tested and evaluated for security weaknesses and vulnerabilities. CSD expects that the marketplace will enable advancements and breakthroughs that will form new paradigms for software development activities. Closing the existing gap not only requires innovative technologies, but also research in software analysis techniques and methods, as well as better awareness of and education about security in the software development process. It is with this approach that CSD expects SWAMP to be a revolutionizing force in the software assurance community for years to come.

SWAMP's unique set of services and capabilities are designed to meet the diverse needs in the software assurance community, and more specifically, address the needs of the following potential users:

1. Software Developers – Improve software development activities by offering a collection of software quality assurance tools and assurance services for software developers to test and evaluate software code for weaknesses and vulnerabilities
2. SQA Tool Developers – Provide tool developers an environment where they can test, calibrate, and improve the coverage area in their tools
3. Software Researchers – Assist software researchers in discovering new techniques and methods to create better performing tools
4. Educators and Students – Provide a learning environment for educators to reinforce core principles and best practices in software development, and provide core essentials to teach students how to develop secure software code

FY 2013 HIGHLIGHTS

- Hosted the NIST Static Analysis Tool Exposition (SATE) V, which is designed to advance research (based on large test sets) of static analysis tools that find security-relevant defects in source code. SATE's purpose is *not* to evaluate or choose the "best" tools. Rather, it is aimed at exploring the following characteristics of tools: relevance of warnings to security, their correctness, and prioritization.
- Successfully integrated with Sonatype, demonstrating SWAMP's ability to automate analysis workflows for a considerable amount of software to support continuous assurance services.
- Demonstrated the ability to handle and process large volumes of different types of software (including open-source software packages, components, and libraries) by executing more than 11,000 packages as part of the integration effort with SONATYPE.
- Transitioned key technologies from the SQA project into SWAMP. These key technologies will be used as part of the SWAMP's tool suite and workflow analysis.
- Successfully integrated and installed five open-source tools (PMD, Findbugs, Cppcheck, Oink, and Clang Static Analyzer) as part of SWAMP's assessment engine.



PERFORMERS

- Morgridge Institute for Research



PROGRAM MANAGER

Kevin.Greene@hq.dhs.gov



TRUSTWORTHY INFRASTRUCTURE

The Trustworthy Infrastructure program focuses on ensuring that the nation's critical infrastructure—such as the power grid, oil and gas pipelines, and the banking and finance sectors—become more secure and less vulnerable to malicious and natural events. This program involves engagement across industry, government, private sector, and academia to improve the core functions of critical sector information systems and control systems in order to protect owners, operators, and users.

In FY 2013, CSD carried out the Trustworthy Infrastructure program through five projects.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID (TCIP-G)

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure which, in turn, depends on the health of an underlying computing and communications network infrastructure that is at serious risk. To address this challenge, CSD and the Department of Energy (DOE) jointly funded the TCIP G project, which aims to significantly improve the way the power infrastructure is built, thus making it more secure, reliable, and safe.

SECURE PROTOCOLS FOR THE ROUTING INFRASTRUCTURE (SPRI)

Routing infrastructure is one of the most critical components of the Internet and other networks, yet it is susceptible to spoofing and other attacks in which malicious actors can redirect users to unsafe websites or pathways. To address this, CSD funds the development of tools and techniques to improve the security of Internet addressing and routing and make them less susceptible to disruption and misdirection.

GF10G12

24300

24250

24200

24150

24100

20

21

22

GFG12



○ **LINKING THE OIL AND GAS INDUSTRY TO IMPROVE CYBERSECURITY (LOGIIC)**

In order to address cybersecurity threats to our nation's critical oil and gas infrastructure and their supervisory control and data acquisition systems, CSD led the creation of the LOGIIC Consortium, an ongoing collaboration between oil and natural gas companies and S&T. The consortium undertakes collaborative research and development (R&D) projects to improve the level of cybersecurity in critical systems of interest to the oil and gas sector.

○ **DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC) DEPLOYMENT INITIATIVE**

The security, trust, and continued functionality of the Internet depends on a more secure, robust DNS. CSD, in partnership with NIST, leads the DNSSEC Deployment Initiative, encouraging all sectors of the digital world to voluntarily adopt measures that will improve the security of the Internet's name infrastructure.

○ **DISTRIBUTED ENVIRONMENT FOR CRITICAL INFRASTRUCTURE DECISION MAKING EXERCISES (DECIDE)**

The nation's financial infrastructure is one of the most lucrative targets for malicious actors. Successful attacks against it could be massively disruptive to the nation's vibrant daily economic activities. To help secure this sector, CSD developed tools that allow finance sector organizations to test their infrastructure and make them more resilient to attacks.



TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID

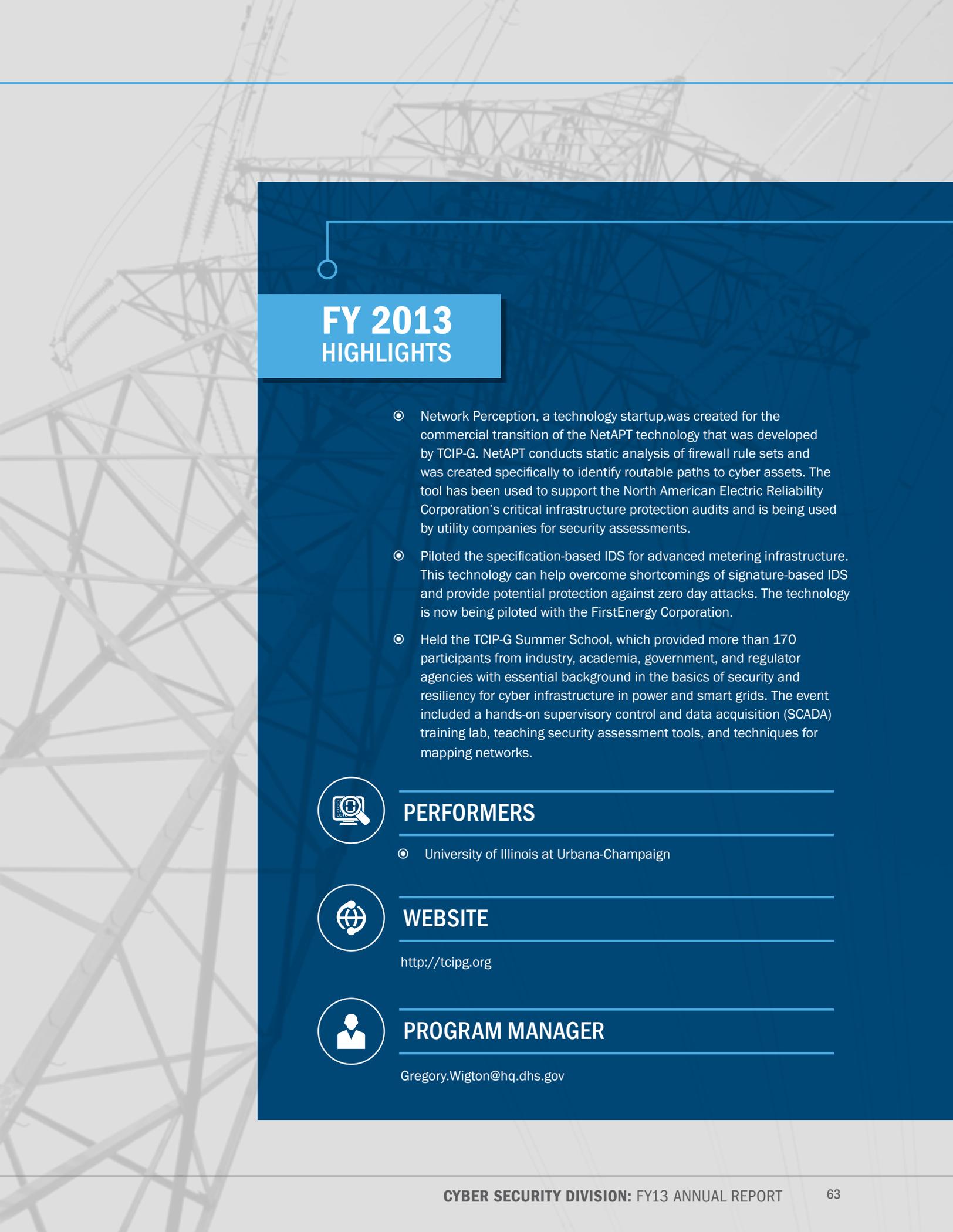
The nation's electric power infrastructure is made up of thousands of utilities, equipment and software vendors, and regulatory agencies including the federal government to develop solutions to prevent network failure risks. These risks may come from cyber hackers who gain access to control networks or create denial-of-service attacks on the networks themselves, or from accidental causes, such as natural disasters or operator errors.

CSD and DOE jointly fund the TCIP-G project to address the challenge of protecting the nation's power grid. Through the project, CSD aims to make a more secure, reliable, and safe power grid by improving the way the grid infrastructure is built. Research conducted as part of the TCIP-G project focuses on securing the low-level devices, communications protocols, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyberattacks, and power emergencies. Simulation

and evaluation techniques are employed to analyze real power grid scenarios and validate the effectiveness of the TCIP-G designs and implementations.

The research from TCIP-G has led to advances in energy control, strengthened access control, and increased customer privacy. Research projects focus on increasing security and reliability at both the device and network level. In addition, TCIP-G has created a simulation and testbed environment that mimics aspects of the power grid, allowing accurate experiments and testing of technologies. TCIP-G has also developed interactive and open-ended applets for middle school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students. Combined, these initiatives provide tools and technologies that will help create a reliable, timely, and secure power grid.





FY 2013 HIGHLIGHTS

- Network Perception, a technology startup, was created for the commercial transition of the NetAPT technology that was developed by TCIP-G. NetAPT conducts static analysis of firewall rule sets and was created specifically to identify routable paths to cyber assets. The tool has been used to support the North American Electric Reliability Corporation's critical infrastructure protection audits and is being used by utility companies for security assessments.
- Piloted the specification-based IDS for advanced metering infrastructure. This technology can help overcome shortcomings of signature-based IDS and provide potential protection against zero day attacks. The technology is now being piloted with the FirstEnergy Corporation.
- Held the TCIP-G Summer School, which provided more than 170 participants from industry, academia, government, and regulator agencies with essential background in the basics of security and resiliency for cyber infrastructure in power and smart grids. The event included a hands-on supervisory control and data acquisition (SCADA) training lab, teaching security assessment tools, and techniques for mapping networks.



PERFORMERS

- University of Illinois at Urbana-Champaign



WEBSITE

<http://tcipg.org>



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



SECURE PROTOCOLS FOR THE ROUTING INFRASTRUCTURE

In 2004, CSD started the SPRI project to improve the security of Internet addressing and routing and make them less susceptible to disruption and misdirection, whether caused maliciously or through misconfiguration. Two particularly vulnerable aspects of the Internet's routing infrastructure are Internet Protocol (IP) addresses and the Border Gateway Protocol (BGP). IP addresses serve as unique identifiers that are critical to the construction of networks and the identification of destinations, while the routing infrastructure relies on the BGP to discover routes between the large networks that make up the Internet. Currently, it is challenging to determine whether IP addresses are authentic and whether a BGP route has been altered, which could allow for the interception or misdirection of traffic.

CSD has played a leading role in the development and promotion of two key standards aimed at addressing these issues: the Resource Public Key Infrastructure (RPKI) standard and the BGPSEC standard. The RPKI standard provides a method for verifying the authenticity of IP addresses and, as of the end of FY13, all existing Regional Internet Registries in the world now use the RPKI standard in production as they certify IP address allocations. The BGPSEC standard allows network operators to detect changes to the routing path, while taking into consideration the scale and complexity of global Internet routing. The systems that support Internet routing and addressing are complex, globally distributed, and owned and operated by a variety of organizations and companies that bear the burden of upgrading

their systems and software to improve security. Because of this, these entities have been involved in every step of the standardization process.

In addition to working with the Internet community to draft the RPKI and BGPSEC standards, CSD is developing tools to encourage the deployment of these technologies by network operators. These tools include an automated test suite that makes it easier for router vendors to test implementation and a tool for creating, validating, and distributing address certificates.



FY 2013 HIGHLIGHTS

- Increased the amount of IPv4 address space that is secured using the RPKI standard by 40 percent.
- Increased the number of participants using the RPKI standard by 50 percent.
- Published four new standards related to RPKI authored by CSD performers, covering management of the protocol, plans for transition in cryptographic algorithms, and validation of routing information. In total, CSD performers have co-authored 75 percent of the standards that define RPKI.
- Held a dozen hands-on, real-time, Internet-live workshops for Internet operators in operator community venues around the world, using CSD-funded implementations of the RPKI standard. Only the CSD-funded implementations support all features of the RPKI standard so as to make the workshops possible.
- Released a CSD-funded implementation of the BGPSEC standard, the first and only available implementation of that standard.



PERFORMERS

- SPARTA Inc.
- Raytheon BBN Technologies



WEBSITE

Open Source suite for RPKI: <http://rpki.net/>

Open Source Relying Party software: <http://sourceforge.net/projects/rpstir/>



PROGRAM MANAGER

Daniel.Massey@hq.dhs.gov



LINKING THE OIL AND GAS INDUSTRY TO IMPROVE CYBERSECURITY

In 2004, DHS identified the oil and gas industry's process control systems (PCSs) and SCADA systems as potential points of threat from terrorists seeking to destabilize the energy industry supply capabilities and the U.S. economy. As legacy systems are connected to operating networks, the attack surface increases significantly, creating vulnerabilities for all owners and operators of infrastructure in the oil and gas industry.

Recognizing this problem, industry and government came together to start the LOGIIC consortium, an ongoing collaboration between CSD and oil and natural gas companies. The LOGIIC consortium facilitates cooperative research, development, testing, and evaluations to improve cybersecurity in petroleum industry digital control systems. The consortium undertakes collaborative R&D projects to improve the level of cybersecurity in critical systems of interest to the oil and gas sector.

LOGIIC represents a model partnership between government and industry. Within the consortium, oil and gas companies contribute the operational environment, expertise, and project management; vendor companies provide security expertise and products; and CSD contributes testing facilities and independent research staff with technical security expertise. The results of LOGIIC research projects drive innovation within oil and gas companies as well as with vendors and suppliers. The end result is not only a more secure infrastructure for the LOGIIC members, but also increased security practices across the industry.

Current members of LOGIIC include BP, Chevron Corporation, Shell, Total SA, and other large, multinational oil and gas companies that operate significant global energy infrastructure.







FY 2013 HIGHLIGHTS

- Completed the Factory Acceptance Testing/Site Acceptance Testing project, which addressed concerns with basic PCSs being delivered to asset owners without proper cybersecurity testing. The final report addressed best standards for acceptance testing based on external standards, previous LOGIIC findings, and current LOGIIC member company specifications for acceptance testing.
- Completed a study on the security of wireless devices within the control systems environment. The study took into account security and security operability in terms of availability, integrity, and confidentiality. The final report discusses the assessment attributes, findings, and considerations for using wireless in process control environments and can be found at <https://logiic.automationfederation.org>.



PERFORMERS

- SRI International



WEBSITE

<https://logiic.automationfederation.org>.



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



DOMAIN NAME SYSTEM SECURITY EXTENSIONS DEPLOYMENT INITIATIVE

The DNS is a critical piece of Internet infrastructure that serves as the Internet’s “phonebook” by translating human-readable host names into IP addresses. Nearly all Internet applications rely on some form of DNS data, and an unintentional error in the DNS can effectively deny service to Internet applications, while intentionally falsified DNS data can result in hijacked communications. For example, erroneous DNS data for SomeBank.com can render SomeBank.com unavailable, while intentionally false data can direct the bank customer to an adversary pretending to be SomeBank.com. The security, trust, and continued functionality of the Internet will be greatly influenced by implementing a more secure, robust DNS. In recent years, the Internet community has developed a standard protocol known as DNSSEC to provide security for all DNS communications. CSD, in partnership with NIST, has led the DNSSEC Deployment Initiative, encouraging all sectors of the digital world to voluntarily adopt measures that will improve the security of the Internet’s naming infrastructure. The initiative is part of a global, cooperative effort involving the public and private sectors.

CSD’s recent DNSSEC efforts revolve around measuring the deployment of DNSSEC technology and monitoring tools to ensure that existing deployments are working as intended. To measure growth in DNSSEC deployment, CSD developed tools to track who is providing DNSSEC data by measuring the number of signed zones and signed delegations. To understand who is making use of the signed data, aggregated

summary reports were added to the DNSSEC Check tool. These reports help measure DNSSEC support in resolvers that are responsible for initiating DNS lookups and ultimately obtaining the DNS records desired by users. To ensure correct operations, tools were also developed to help manage deployments. This work includes multiple troubleshooting and monitoring tools to provide better situational awareness for DNS operators, monitoring plug-ins that add DNSSEC capabilities to existing network monitoring systems, and DNSSEC-Nodes tools that observe DNS packets “on the wire,” as well as other tools that provide DNS operations support, such as “out-of-band” signing, zone realms, and threshold-based auto signing.

FY 2013 marked the final year of funding for the DNSSEC Deployment Initiative and culminated a significant effort to create a trust infrastructure for the Internet. Through the development of the DNSSEC protocol, public approval of the protocol through the Internet governance bodies, outreach to the operations community, and development of tools for developers and administrators, the DNSSEC Deployment Initiative has built an infrastructure that will help secure transactional activities across the Internet.



FY 2013 HIGHLIGHTS

- ⦿ Enabled DNSSEC on 85 percent of U.S. government websites (i.e., sites with a .gov domain).
- ⦿ Achieved full support from Google Public DNS for DNSSEC validation.
- ⦿ Signed a memorandum of understanding that transitioned DNSSEC Deployment Initiative efforts to the Internet Society.



PERFORMERS

- ⦿ Shinkuro Inc.
- ⦿ SPARTA Inc.
- ⦿ NIST



PROGRAM MANAGER

Edward.Rhyne@hq.dhs.gov



DISTRIBUTED ENVIRONMENT FOR CRITICAL INFRASTRUCTURE DECISION MAKING EXERCISES

In late 2005, a risk manager in a large New-York brokerage authored a short white paper calling for technologies that would assist financial institutions in better understanding risks associated with disruption of, and changes to, end-to-end transaction processing. The paper concluded that most financial enterprises understand the routine sources of risk to their business and take adequate steps to mitigate them, such as planning for disruptions that impact their own business, whether directly or through another party in their immediate value chain. However, as financial transactions become more closely integrated, interconnected, and efficient, and the Securities and Exchange Commission mandates shorter deadlines for completing transactions, risk managers are increasingly concerned with business disruptions resulting from remote events—those that originate outside the enterprise’s typical span of operational control, awareness, or influence.

These disruptions include events like 9/11, the 2003 blackout in the Northeast, and the terrorist threat against New-Jersey-based financial institutions in late 2002. The latter event resulted in DHS declaring an alert condition “Orange” for the finance sector.

Given the potential threat to this infrastructure, CSD and the finance sector collaborated to identify the need for a configurable computer-based toolkit, or suite of test applications, that allows finance sector organizations to test their concept of operations either individually or with

other finance sector entities. These tests will help organizations address risk management, develop attack responses, and prepare proactive measures that will help deter future attacks and system failures.

This collaboration resulted in the award of the DECIDE contract, which produced a prototype of a national cyber war-gaming capability designed to make critical infrastructure more resilient to cyberattacks. The prototype tool was used for two demonstrations to the government and finance sector in 2012 and 2013 and is intended for use by organizations involved in the trading of equities in the U.S. stock market.

This initial prototype can deliver simulation-supported cyber exercises to the desktops of critical infrastructure owners and operators, enabling them to create and run extremely cost-effective exercises that are valuable and relevant to their own business interests. Organizations that use the technology product will be able to strengthen their incident response plans and their ability to execute these plans under conditions of operational duress.



FY 2013 HIGHLIGHTS

- Deployed DECIDE in Quantum Dawn 2, a cyber exercise hosted by the U.S. Securities Industry and Financial Markets Association. The goal was to test incident response plans for both the finance sector and individual firms. The exercise included more than 50 participants from the finance sector.



PERFORMERS

- Norwich University



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



TRANSITION AND OUTREACH

The Transition and Outreach program accelerates the transition of new and existing cybersecurity technologies, including open-source solutions, into commercial products and services. The program uses robust internal assessments, evaluations, pilots, and experiments to speed up this transition to the commercial marketplace.

In FY 2013, CSD carried out the Transition and Outreach program across four projects.

○ **TRANSITION TO PRACTICE (TTP)**

Transitioning new technologies out of the research lab and into the commercial marketplace can be a difficult task. CSD is working to identify and introduce mature technologies to a wider audience by building upon CSD's successful transition model.

○ **EXPERIMENTS AND PILOTS**

There are many challenges to facilitating technology transition to both public and private customers, and the opportunity for testing and evaluation is not always readily available. CSD provides a platform for experimentation, testing, evaluation, and operational deployment to facilitate more efficient technology transfer.

○ **CYBERSECURITY ASSESSMENT AND EVALUATION**

Regardless of their quality and potential, many R&D projects are jeopardized due to the lack of proper end user assessment. To avoid this pitfall, CSD conducts third party evaluations for selected CSD funded R&D projects. These evaluations are conducted from the user's perspective and help CSD program managers and project performers assess the performance of technology solutions and products. CSD offers the ability to better assess the performance of technologies by conducting third party evaluations from the user's perspective.

○ **HOMELAND OPEN SECURITY TECHNOLOGY (HOST)**

Government's extensive IT infrastructure is often slow to adapt to ever changing cybersecurity threats, due in part to a lack of collaboration. The HOST project was established to increase government awareness of open security methods, models, and technologies that provide sustainable approaches to support national cybersecurity objectives.



TRANSITION TO PRACTICE

The technology “valley of death” is a well-known concept in the R&D community. The term succinctly describes the historically difficult task of transitioning technology out of the research lab and into the commercial marketplace. The purpose of the TTP project is to build a bridge over the “valley of death.”

In 2011, the Networking and Information Technology Research and Development (NITRD) program of the White House named ways the federal government can rapidly improve the security of the nation’s cyber infrastructure. From that list, one of the NITRD program’s top priorities is to accelerate the transition of cybersecurity research into widespread deployment and use via the marketplace. Since DHS is one of the agencies designated to address this priority, CSD established the TTP project. TTP builds on CSD’s previous successes in transitioning cybersecurity technologies into commercially available products.

In accordance with the NITRD program’s recommendations, TTP’s goals are to: (1) identify mature technologies that address an existing or imminent cybersecurity gap in public or

private systems that impact national security; (2) fund test and evaluation and operational pilots for these technologies; and (3) introduce cybersecurity technology throughout the HSE through partnerships and commercialization.

TTP targets technologies that are most likely to successfully transition to the commercial market within two years and that will have a notable impact on the cybersecurity of our nation’s networks or systems. Additionally, TTP will provide a connection point for cybersecurity researchers, the federal government, and the private sector and ensure technology transitions from the research lab to the HSE.

In FY 2013, technology foraging efforts focused on federally funded research conducted at the DOE national laboratories and DOD-affiliated research labs. Technology foraging discovers, adapts, and leverages technology solutions developed by other governmental and private-sector entities to address risks to our security. In subsequent years, foraging activities will expand to DOD research centers and academic institutions.





FY 2013 HIGHLIGHTS

- ⦿ Reviewed 60 federally funded cybersecurity technologies at seven DOE national laboratories and three DOD-affiliated labs and selected nine promising technologies to transition.
- ⦿ Expanded existing partnerships and initiated new partnerships with numerous federal agencies, federal R&D organizations, critical infrastructure operators, and the private sector.
- ⦿ Held four Technology Demonstration Day Events to showcase the project's first eight technologies to the federal government, finance sector and investors, systems integrators, and IT companies.



PERFORMERS

- ⦿ Sandia National Laboratories
- ⦿ SRI International

R&D PARTNERS

- ⦿ Johns Hopkins University – Applied Physics Laboratory
- ⦿ Lawrence Livermore National Laboratory
- ⦿ Los Alamos National Laboratory
- ⦿ Massachusetts Institute of Technology – Lincoln Laboratory
- ⦿ Oak Ridge National Laboratory
- ⦿ Pacific Northwest National Laboratory
- ⦿ Sandia National Laboratories
- ⦿ SPAWAR Systems Center – Pacific



PROGRAM MANAGER

Michael.Pozmantier@hq.dhs.gov



EXPERIMENTS AND PILOTS

Technology transfer from the lab to the marketplace is a vital and unique aspect of CSD's R&D efforts. A platform or opportunity for experimental deployment, testing, and evaluation is not always readily available, and there are many challenges to facilitating technology transition to both public and private customers. Furthermore, DHS leadership and operational components, such as the DHS Chief Information Officer (CIO), Federal Law Enforcement Training Center, and DHS Office of Cybersecurity and Communications, need opportunities to test the operational capabilities of new technologies.

The Experiments and Pilots project provides a platform for experimentation, testing, evaluation, and operational deployment to facilitate technology transfer. Deploying CSD-developed technologies allows operational components to better understand cutting-edge capabilities. The first step is to identify mature technologies that were developed by CSD and are ready for experimentation, piloting, or deployment in an operational environment. Once a list of technologies is identified, CSD meets with customers and operational components to determine which technologies could be deployed in their operational networks. The goal is to place CSD-funded technologies into the network environments of our customers and partners to enhance their security posture and receive feedback on the products.

By piloting mature technologies, CSD is providing transition opportunities for funded performers and also filling the operational needs of division's end-users. Other government organizations are able to pilot technologies they may not have known about or that they may not have been able to fund themselves. CSD-funded performers also receive valuable feedback on their technology, allowing them to make improvements before the technology becomes commercially available. Successful deployments will lead to the adoption of the technology by the customer and full deployment to the HSE.

FY 2013 HIGHLIGHTS

- Piloted the VIAssist network visualization tool technology with the Library of Congress. VIAssist helps analyze network traffic and security event data by providing scalable, visual representations of cyber data.
- Piloted a central Identity and Access Management (IAM) infrastructure that controls physical and logical access decisions based on policies and access rules with the DC Office of the Chief Technology Officer.
- Piloted CLIQUE and Traffic Circle network behavior analysis applications with DHS, S&T and CIO over a four-month period. The applications provide computer network traffic analysis and visualization and were partially funded by CSD through DOE. At the end of the pilot, the goal is to integrate these tools into permanent operations.



PERFORMERS

- Pacific Northwest National Laboratory
- Queralt Inc.



PROGRAM MANAGER

Gregory.Wigton@hq.dhs.gov



CYBERSECURITY ASSESSMENT AND EVALUATION

Despite the large amount of R&D funding spent every year, successful placement of technologies into the hands of end users is a challenge, thus jeopardizing the significant investments federal R&D organizations make.

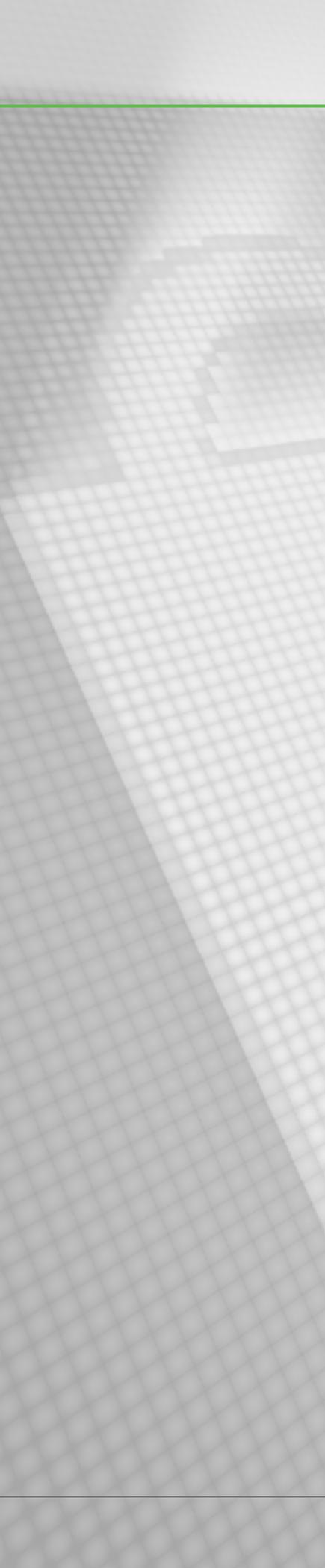
To address this gap, the Cybersecurity Assessment and Evaluation project provides CSD the ability to better assess the performance of technologies developed under its sponsorship, more effectively collect end-user requirements, validate R&D technical topic areas, quickly mobilize technology into the hands of practitioners in the field, and increase the rates of commercialization success.

In order to accurately assess CSD-funded technologies, the project uses a multi-faceted evaluation approach. One aspect of this approach

is to conduct adversarial or “red team” testing of CSD technologies. Evaluations are also conducted from the user perspective and the resulting analysis reports provide meaningful feedback to the respective development teams to improve the usability of their product, increasing its chances for adoption or “lodgment” within the end-user community.

Additionally, the project builds collaborative models to promote cyber innovation and awareness, entrepreneurship, and investment among the cybersecurity stakeholder community, primarily through the Security Innovation Network (SINET). SINET events bring together leaders and innovators from industry, academia, and government to advance successful public-private engagement and partnerships.





FY 2013 HIGHLIGHTS

- Completed a red team analysis of the Secure Network Attribution and Prioritization (SNAP) protocol. Information received during the course of the analysis enabled the SNAP development team to correct issues and provided valuable implementation considerations.
- Supported three SINET events, including the October 2012 SINET Showcase in Washington, D.C., the 2013 SINET Innovation Summit in New York City, and the 2013 SINET IT Security Entrepreneurs' Forum in Palo Alto, California.
- Completed testing of the Code Dx static analysis tool.



PERFORMERS

- Exelis Inc.
- Sandia National Laboratories



PROGRAM MANAGER

Scott.Tousley@hq.dhs.gov



HOMELAND OPEN SECURITY TECHNOLOGY

Despite the rapid increase in cybersecurity threats to the HSE, the government's IT infrastructure is expansive and often slow to adapt. Additionally, the transition of cybersecurity innovation from government research to the marketplace remains challenging.

To combat these complex issues, the HOST project was established and is leading the government in increasing awareness of open security methods, models, and technologies that provide sustainable approaches to support national cybersecurity objectives. Open security is the application of open-source software (OSS) approaches to help solve cybersecurity problems. In short, open security improves security through collaboration.

This project continues to investigate opportunities and challenges in the government's adoption and application of OSS; seed investments in various OSS technologies relevant to improving cybersecurity; maintain an inventory and support the discovery of open security technologies; establish an open security community; and support outreach creating intersections between the government, open-source, and open security communities. From these efforts, HOST's impacts will be to provide affordable, adaptable, accessible, and timely OSS-based cybersecurity innovation and alternate approaches for the commercialization of government-funded cybersecurity research.





FY 2013 HIGHLIGHTS

- Published and publicly briefed the “Open Source Software in Government: Challenges and Opportunities” report.
- Transitioned the OSS-based, multi-threaded IDS Suricata.



PERFORMERS

- Georgia Tech Research Institute



PROGRAM MANAGER

Daniel.Massey@hq.dhs.gov

PERFORMER INDEX

PERFORMER	PRIME CONTACT INFORMATION	PROJECT	ROLE
ATC-NY	Rob Joyce (rjoyce@atcorp.com)	Secure Cloud Computing	Silverline
Basis Technology	Brian Carrier (brianc@basistech.com)	Cybersecurity Forensics	Enabling Law Enforcement With Open Source Digital Forensics Software
Berla Corporation	Ben LeMere (blemere@berlacorp.com)	Cybersecurity Forensics	GPS Forensic Logical Analysis Tool - Blackthorn3
Berla Corporation	Ben LeMere (blemere@berlacorp.com)	Cybersecurity Forensics	Project iVe
Brigham Young University	Sean Warnick, PhD. (sean.warnick@gmail.com)	Internet Measurement and Attack Modeling	Attack Modeling for Distributed Decision Architectures
Carnegie Mellon University	Nicolas Christian (nicolasc@cmu.edu)	Cyber Economic Incentives	Understanding and Disrupting the Economics of Cybercrime
Carnegie Mellon University	Randy Trzeciak (rft@cert.org)	Insider Threat	Banking and Finance Sector Insider Threat Study
Columbia University	Salvatore Stolfo, PhD. (Sal@cs.columbia.edu)	Internet Measurement and Attack Modeling	Advanced Situation Awareness of High Impact Malware Attacks Against the Internet Routing Infrastructure
Council on CyberSecurity	Karen Evans (karenevans@prodigy.net)	Cybersecurity Competitions	US Cyber Challenge (USCC)
Dartmouth College	Shari Lawrence Pfleeger (pfleeger@dartmouth.edu)	Incident Response Communities	Research Director
Def-Logix	Paul Rivera (privera@def-logix.com)	Moving Target Defense	Hardware-Enabled Zero Day Protection (HEZDP)
Endeavour Systems	Will Hickie (will.hickie@endeavorsystems.com)	Moving Target Defense	Multi-layer Ever-changing Self-defense Service (MESS)
Exelis Inc.	Adam Hovak (Adam.Hovak@exelisinc.com)	Cybersecurity Assessment and Evaluation	
Exelis Inc.	Adam Hovak (adam.hovak@exelisinc.com)	Cybersecurity Forensics	Law Enforcement Information Portal - CyberFETCH
Exelis Inc.	Rosanne Pelli (Rosanne.pelli@exelisinc.com)	Tailored Trustworthy Spaces	Evidentiary Integrity for Incident Response
George Mason University	Sushil Jajodia (jajodia@gmu.edu)	Enterprise Level Security Metrics	Metrics Suite for Enterprise-Level Attack Graph Analysis
George Mason University	Sub-Contractor to Dartmouth College	Incident Response Communities	
Georgia Tech Research Corporation	Wenke Lee, PhD. (Wenke@cc.gatech.edu)	Internet Measurement and Attack Modeling	Comprehensive Understanding of Malicious Overlay Networks
Georgia Tech Research Institute	Joshua Davis (Joshua.Davis@gtri.gatech.edu)	Homeland Open Security Technologies	Project Lead
Global Cyber Risk LLC	Jody Westby (westby@mindspring.com)	Research Data Repository	Legal Framework and Privacy Support

PERFORMER	PRIME CONTACT INFORMATION	PROJECT	ROLE
Hewlett-Packard Company	Sub-Contractor to Dartmouth College	Incident Response Communities	
HRL Laboratories LLC	Aleksey Nogin (anogin@hrl.com)	Secure Cloud Computing	Cloud-COP
HRL Laboratories LLC	Aleksey Nogin (anogin@hrl.com)	Software Quality Assurance	Tunable Information Flow
IBM	Larry Koved (koved@us.ibm.com)	Usable Cybersecurity	Usable Multi-Factor Authentication and Risk-Based Authorization
IBM T.J. Watson Research Center	Dimitrios Pendarakis (dimitris@us.ibm.com)	Moving Target Defense	Hardware Based Malware Defenses and End-to-End Trust
Indiana University	Jean Camp (ljcamp@indiana.edu)	Usable Cybersecurity	CUTS: Coordinating User and Technical Security
Johns Hopkins University - Applied Physics Laboratory	Maria Vachino (maria.vachino@jhuapl.edu) Tom Smith (tom.smith@jhuapl.edu)	Identity and Access Management	Host the Identity Management Testbed; Backend Attribute Exchange
Kestrel Technologies	Dr. Henny Sipma (sipma@kestreltechnology.com)	Software Quality Assurance	A Gold Standard for Benchmarking C Source Code Static Analysis Tools
Massachusetts Institute of Technology	Dr. Lalana Kagel (lkagal@CSAIL.MIT.EDU)	Data Privacy Technologies	Accountable Information Usage in Distributed Information Sharing Environments
Merit Networks, Inc.	W. Joseph Adams, PhD. (Wjadams@merit.edu)	Internet Measurement and Attack Modeling	Enabling Operational Use of RPKI via Internet Routing Registries
MITRE Corporation	Stuart Shapiro (sshapiro@mitre.org)	Data Privacy Technologies	Privacy Enhancing Technology Engineering and Transition
Morgridge Institute for Research	Miron Livny (miron@cs.wisc.edu)	Software Assurance Marketplace (SWAMP)	SWAMP
National Institute of Standards and Technology	Barbara Guttman (barbara.guttman@nist.gov; cftt@nist.gov; and nsrl@nist.gov)	Cybersecurity Forensics	National Software Reference Library/ Cyber Forensics Tool Testing
Naval Postgraduate School	Cynthia Irvine, PhD. (Irvine@nps.edu)	Internet Measurement and Attack Modeling	Methodology for Assessment of Security Properties
Naval Postgraduate School	Robert Beverly, PhD. (Rbeverly@nps.edu)	Internet Measurement and Attack Modeling	High-Frequency Active Internet Topology Mapping
Naval Postgraduate School	Simson Garfinkel (sgarfin@nps.edu)	Cybersecurity Forensics	Gaming Systems Forensics
Naval Postgraduate School	Simson Garfinkel (sgarfin@nps.edu)	Insider Threat	Detecting Threatening Insiders with Lightweight Media Forensics
Northrop Grumman	Donald Steiner (Donald.Steiner@ngc.com)	Insider Threat	Monitoring DBMS Activity for Detecting Data Exfiltration by Insiders

PERFORMER INDEX

PERFORMER	PRIME CONTACT INFORMATION	PROJECT	ROLE
Northrop Grumman Information Systems	Jeffrey Foley (Jeffrey.I.foley@ngc.com)	Moving Target Defense	Appliance for Active Repositioning in Cyberspace (AARC)
Norwich University	Phil Susmann (susmann@norwich.edu)	Distributed Environment for Critical Infrastructure Decision Making Exercises (DECIDE)	Distributed Environment for Critical Infrastructure Decision Making Exercises (DECIDE)
Oak Ridge National Laboratory	John Goodall, PhD. (Jgoodall@ornl.gov)	Internet Measurement and Attack Modeling	Visually Fusing Contextual Data for Situational Understanding
Pacific Northwest National Laboratory	Christopher S. Oehmen (christopher.oehmen@pnnl.gov)	Tailored Trustworthy Spaces	Nature Inspired Health (LINEBACKER)
Pacific Northwest National Laboratory	Daniel M. Best (daniel.best@pnnl.gov)	Experiments and Pilots	Principal Investigator
Pacific Northwest National Laboratory	Daniel M. Best (daniel.best@pnnl.gov)	Internet Measurement and Attack Modeling	Scalable Modeling of Network Flows for US-CERT (Traffic Circle/CLIQUE)
Packet Clearing House (PCH)	Bill Woodcock (woody@pch.net)	Research Data Repository	Data Host and Dat Provider
Parsons Engineering	Sandy Murphy (Sandra.Murphy@parsons.com)	Secure Protocols for the Routing Infrastructure (SPRI)	Standards Development & System Prototyping
PIVPointe	Duane Stafford (duane @pivpointe.com)	Identity and Access Management	Principal Investigator
Princeton University	Ruby Lee (rblee@princeton.edu)	Moving Target Defense	Using Moving Target Defense for Secure Hardware Design
Queralt Inc.	Michael Queralt (michaelq@queraltinc.com)	Experiments and Pilots	Small Business Innovation Research effort "Attribute Based Authorization & Visitor Application"
Queralt Inc.	Michael Queralt (michaelq@queraltinc.com)	Identity and Access Management	Small Business Innovation Research effort "Attribute Based Authorization & Visitor Application"
Raytheon BBN Technologies	Sub-Contractor to Parsons Engineering	Secure Protocols for the Routing Infrastructure (SPRI)	Standards Development & System Prototyping
Raytheon BBN Technologies	Ronald Watro, PhD. (Rwatro@bbn.com)	Internet Measurement and Attack Modeling	Real-time Protocol Shepherds (RePS)
Red Balloon Security, Inc.	Salvatore Stolfo, PhD. (sal@redballoonsecurity.com)	Internet Measurement and Attack Modeling	Host-based defense of Cisco IOS routers using Software Symbiotes
Research Triangle Institute International	Charlotte Scheper (cscheper@rti.org)	Research Data Repository	Coordination Center Operations
Rutgers University	Nina Fefferman (feffermn@dimacs.rutgers.edu)	Tailored Trustworthy Spaces	Bio-Inspired Distributed Decision Algorithms for Anomaly Detection
S34A Inc.	Hank Wallace (hwallace@s34a.com)	Cybersecurity Forensics	Solid State Storage Investigative Tools for Law Enforcement
Sandia National Laboratories	Kandy Phan (kphan@sandia.gov)	Cybersecurity Assessment and Evaluation	Performer

PERFORMER	PRIME CONTACT INFORMATION	PROJECT	ROLE
Sandia National Laboratories	Susanna Gordon (spgordo@sandia.gov)	Transition to Practice	Test and Evaluation
Secure Decisions	Ken Prole (Ken.Prole@avi.com)	Software Quality Assurance	Code Dx
Shinkuro Inc.	Steve Crocker (Steve@shinkuro.com)	Domain Name System Security Extensions Deployment Initiative (DNSSEC)	Domain Name System Security (DNSSEC) Protocol Development
Space and Naval Warfare Systems Center Atlantic	Richard Kaye (richard.kaye@navy.mil)	Identity and Access Management	Principal Investigator
SPARTA Inc.	Russ Mundy (Russ.Mundy@sparta.com)	Domain Name System Security Extensions Deployment Initiative (DNSSEC)	Ubiquitous Deployment of Domain Name System Security
SRI International	Ulf Lindqvist (ulf.lindqvist@sri.com)	Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC)	Project Management
SRI International	Dave Ballinson (david.balenson@sri.com)	Identity and Access Management	FIVICS - Finance Sector pilot support
University of Alabama at Birmingham	Ragib Hasan (ragib@cis.uab.edu)	Tailored Trustworthy Spaces	Secure Location Provenance for Mobile Devices
University of California - Berkeley, International Computer Science Institute (USC - ICSI)	Nicholas Weaver, PhD. (nweaver@ICSI.Berkeley.edu)	Internet Measurement and Attack Modeling	Netalzyr NG: Monitoring DNS, DNSSEC, and TLS from the Edge
University of California - San Diego, Cooperative Association for Internet Data Analysis (CAIDA)	K. Claffy, PhD. (Kc@caida.org)	Internet Measurement and Attack Modeling	Cartographic Capabilities for Critical Cyber Infrastructure
University of California, San Diego (UCSD)	Kimberly ("kc") Claffy (kc@sdsc.edu)	Research Data Repository	Data Host and Dat Provider
University of Houston	Weidong (Larry) Shi (larryshi@cs.uh.edu)	Usable Cybersecurity	Implicit and Continuous Mobile User Identification/Authentication Using Smartphone Sensors
University of Illinois, Urbana-Champaign (UIUC)	Bill Sanders (whs@illinois.edu)	Trustworthy Cyber Infrastructure for the Power Grid (TCIP-G)	Project Director
University of Illinois, Urbana-Champaign (UIUC)	David Nicol (dmnicol@illinois.edu)	Enterprise Level Security Metrics	A Tool for Compliance and Depth of Defense Metrics
University of Maryland	Larry Gordon (lgordon@rhsmith.umd.edu)	Cyber Economic Incentives	Reducing The Challenges to Making Cybersecurity Investments in the Private Sector
University of Michigan	Michael Bailey (mibailey@eecs.umich.edu)	Research Data Repository	Data Host and Dat Provider

PERFORMER INDEX

PERFORMER	PRIME CONTACT INFORMATION	PROJECT	ROLE
University of Michigan	Mingyan Liu (mingyan@umich.edu)	Cyber Economic Incentives	Towards a Global Network Reputation System: A Mechanism Design Approach
University of North Carolina at Chapel Hill	Fabian Monrose (fabian@cs.unc.edu)	Tailored Trustworthy Spaces	Efficient Tracking, Logging and Blocking of Accesses to Digital Objects
University of Southern California, Information Sciences Institute (USC-ISI)	John Heideman (johnh@isi.edu)	Research Data Repository	Data Host and Data Provider
University of Southern California, Information Sciences Institute (USC-ISI)	John Heidenmann, PhD. (johnh@isi.edu)	Internet Measurement and Attack Modeling	The Retrospective Future in the Internet (Retro-Future)
University of Southern California, Information Sciences Institute (USC-ISI)	Terry Benzel (tbenzel@isi.edu)	Experimental Research Testbed	Testbed Development and Operation
University of Texas - San Antonio (UTSA)	Greg White (Greg.White@utsa.edu)	Cybersecurity Competitions	National Collegiate Cyber Defense Competition (NCCDC)
University of Washington, Applied Physics Laboratory	Dave Dittrich, PhD. (dittrich@u.washington.edu)	Internet Measurement and Attack Modeling	From Local to Global Awareness: A Distributed Incident Management System (DIMS)
University of Wisconsin	Paul Barford (pb@cs.wisc.edu)	Research Data Repository	Data Provider
viaForensics	Andrew Hoog (ahoog@viaforensics.com)	Cybersecurity Forensics	NAND/NOR Chip Forensics

