Cyber Security Division

FY 2011 Annual Report

Homeland Security

Science and Technology

LETTER FROM THE DIRECTOR

Today, the challenges faced in cybersecurity are perhaps some of the most difficult of our time. Information technology (IT) has become crucial to the essential functions of daily life — from commerce and the provision of goods and services to research and innovation. It promotes economic development by opening access to new markets, facilitates the organization and delivery of humanitarian assistance, and supports the functions of critical civil, public safety, and national security infrastructures. And, as evidenced by world events over the past year, it has also become a key tool in ensuring the free flow of information between individuals, organizations, and governments in ways that few could have foreseen only a few years ago.

As dependence on the Internet has grown, so, too, have the security risks associated with that dependency. The reliable functioning of national and global networks, and the integrity of the information that travels over the Internet, are threatened by a wide range of activities. These threats are increasing in sophistication and gravity and have many sources.

Whatever the source of the cyber threat, however, defending against it is a key priority of both the Obama administration, which has directed the implementation of a comprehensive domestic strategy to address cyber vulnerabilities, and the Department of Homeland Security (DHS), which identified safeguarding and securing cyberspace as one of its top five priorities in the 2010 Quadrennial Homeland Security Review (QHSR).

The DHS Science and Technology Directorate's (S&T) Cyber Security Division (CSD) has an essential role in support of this vital mission through the development and implementation of an aggressive cybersecurity research agenda encompassing the full lifecycle of technology — research, development, test, evaluation and transition to practice.

Our key objectives are to

- develop and transition new technologies, tools, and techniques to protect and secure systems, networks, infrastructure, and users, improving the foundational elements of our nation's and the world's critical and information infrastructures; and
- provide coordination and research and development leadership to improve research infrastructure and strengthen the security of the nation's IT infrastructure. This includes working with DHS components, agencies of the U.S. government, private-sector partners and stakeholders, international partners, academia, and the national and industry laboratories.

Fiscal Year 2011 (FY 2011) was a busy and productive year for CSD. In addition to being created as a division within S&T's Homeland Security Advanced Research Projects Agency (HSARPA), we also had a number of noteworthy highlights, including the following:

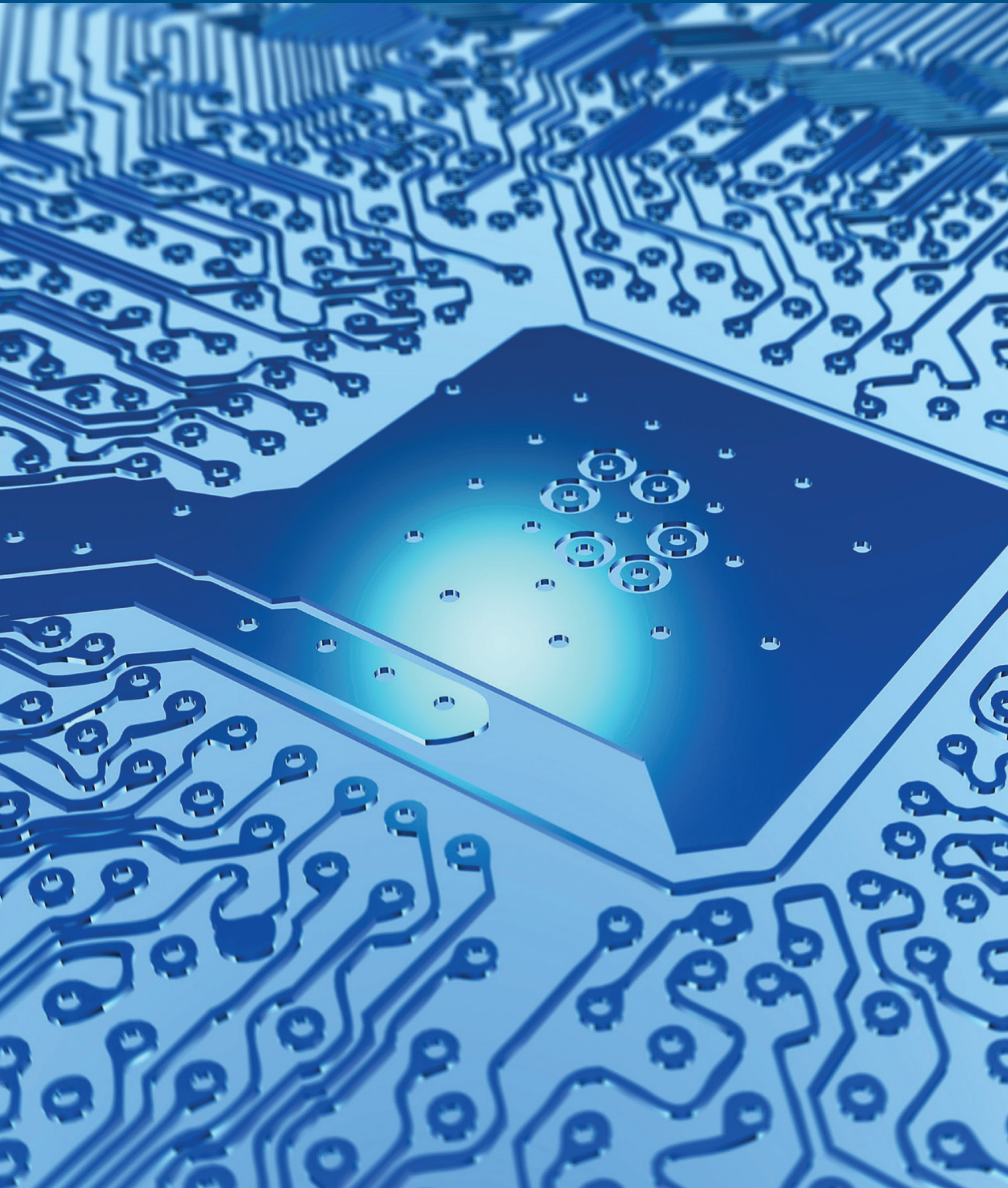
- Contributing to the development of Trustworthy Cyberspace: Strategic Plan for Federal Cybersecurity Research and Development Program, which was released by the White House Office of Science and Technology Policy in December 2011;
- Contributing to the development of the Blueprint for a Secure Cyber Future, which was released by DHS in November 2011;
- Releasing a Broad Agency Announcement solicitation seeking proposals aimed at improving security in both federal networks and the larger Internet, and developing new and enhanced technologies for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure, resulting in more than 1,000 white papers and more than 200 full proposals;
- Receiving a National Cybersecurity Innovation Award at the Sans Institute's Second Annual National Cybersecurity Innovation Conference for the division's Domain Name System Security Extensions (DNSSEC) Deployment Initiative; and
- Releasing the first prototype of the First Responder Cyber Field Kit, which will aid non-technical law enforcement officers in the quick investigation and extraction of evidence from computers and other USB-enabled devices, to twenty federal, state and local agencies for a six-month testing period.

This annual report will give you a high-level understanding of CSD's FY 2011 programs and projects and an overview of their accomplishments. I encourage you to visit the CSD website at www.cyber.st.dhs.gov or to reach out to the CSD program managers listed in this report for more information.

Douglas Maughan

Douglas Maughan, Ph.D.
Cyber Security Division Director

TABLE OF CONTENTS



CYBER SECURITY DIVISION OVERVIEW

In Fiscal Year 2011 (FY 2011), the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate established the Cyber Security Division (CSD), within the Directorate's Homeland Security Advanced Research Projects Agency (HSARPA), in response to the increasing importance of the cybersecurity mission. CSD's mission is to develop and transition new technologies, tools, and techniques to protect and secure systems, networks, infrastructure, and users, improving the foundational elements of our nation's critical infrastructure and the world's information infrastructure; and, to provide coordination and research and development leadership across federal, state, and municipal government; international partners; the private sector; and academia to improve cybersecurity research infrastructure.

CSD's work serves a wide range of customers by coordinating and cooperating with partners within the Department and at other federal agencies; state and municipal administrations and first responders; private-sector companies in a wide range of industries; Internet security researchers around the world; and universities and national laboratories.

To accomplish its mission and serve its customers, CSD has organized its work into five major program areas:

- ***Research Infrastructure to Support Cybersecurity (RISC)*** — provides a national and international-level research infrastructure to enable the cybersecurity research community to discover, test, and analyze state-of-the-art tools, technologies, and software in a scientifically rigorous and ethical manner.
- ***Trustworthy Cyber Infrastructure (TCI)*** — focuses on ensuring that the nation's critical infrastructure — such as the oil and gas pipelines, information infrastructure, and the Internet — become more secure and less vulnerable to malicious and natural events.
- ***Foundational Elements of Cyber Systems (FECS)*** — focuses research and development (R&D) activities on the characteristics that are essential to the desired end-states of trustworthy cyber systems and accelerates the transition of new cybersecurity technologies into commercial products and services.
- ***Cybersecurity User Protection and Education (CUPE)*** — focuses R&D activities on developing ways to help all types of users — from improving the security and protection of user online activity, to attracting the next generation of cybersecurity warriors, to providing the tools needed for investigating cyber criminal and terrorist activity.
- ***Cybersecurity Technology Evaluation and Transition (CTET)*** — provides a coordinated process of assessments, evaluations, and operational experiments and pilots to transition the fruits of research into practice.

RESEARCH INFRASTRUCTURE TO SUPPORT CYBERSECURITY

About This Program

Cybersecurity R&D involves understanding new threats and risks, and discovering solutions that will help protect our nation's cyber infrastructure. The Research Infrastructure to Support Cybersecurity (RISC) program provides a national and international research infrastructure to enable 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 U.S.-based computer networks and systems.

In FY 2011, S&T carried out the RISC program through two projects:

- ***Experimental Research Testbed*** — S&T provides a cybersecurity testbed capable of large-scale, repeatable experiments to safely analyze cyber attacks, evaluate defense mechanisms against attacks on the cyber infrastructure, and develop attack mitigation and confinement strategies.
- ***Research Data Repository*** — S&T created and maintains a large-scale data set repository of real network and system traffic to support the cybersecurity research community in its mission to accelerate the design, production, and evaluation of next-generation cybersecurity solutions, including commercial products.

Experimental Research Testbed

The Experimental Research Testbed Project focuses on providing cybersecurity researchers the ability to run experiments on a secure “virtual Internet.” The testbed provides contained environments that allow researchers to safely test advanced defense mechanisms against “live” threats without endangering other research or the larger Internet. The project began in 2004 with the creation of the Defense Technology Experimental Research (DETER) testbed and was originally jointly funded with the National Science Foundation (NSF). The DETER testbed is used to test and evaluate cybersecurity technologies by more than 200 organizations from more than 20 states and 17 countries, including major DHS-funded researchers, government, industry, academia, and educational users. Additionally, the DETER testbed has been used by more than 40 classes, from 30 institutions and involving more than 2,000 students.

The DETER testbed provides the necessary infrastructure — networks, tools, methodologies, and supporting processes — to support national testing of emerging and advanced security technologies. Current efforts will support larger and more complex experiments with increased usability.

The success of the DETER testbed lies largely on its collaboration with the cybersecurity research community. Annual workshops are conducted to disseminate and discuss project results and outcomes, and reports documenting benchmarks, testbeds, data collection and analysis, and evaluations of security mechanisms that have been deployed.

FY 2011 Highlights

- A complete redesign of the tools and techniques used to create, manage, and analyze experiments, allowing better abstraction and quicker testing of concepts, thereby resulting in faster iterations toward a solution. Development will be finalized and deployment of this new approach will occur in FY 2012.
- The DETER testbed software was successfully installed on a cluster of machines at the University of Illinois at Urbana-Champaign (UIUC), expanding the reach of the testbed and eventually allowing federated access to unique Process Control System equipment physically located at UIUC.
- The process through which experiments are provisioned with computing resources was dramatically improved, allowing significantly larger experiments. The previous approach required a server for each computer represented in an experiment, limiting the size of experiments to the total number of servers in the testbed, 400. The new approach allows a single server to operate as multiple computers, using a technology called virtualization. This makes experiments with hundreds of thousands of nodes possible. The number of computers a server can represent is automatically configured; the number is based upon the amount of work each virtualized computer will be performing.

Project Performers

- University of Southern California – Information Sciences Institute (USC-ISI)
- University of California, Berkeley (UC – Berkeley)
- Pacific Northwest National Laboratory (PNNL)
- University of Illinois at Urbana-Champaign (UIUC)

Website

www.deter-project.org

Program Manager

Luke Berndt, luke.berndt@hq.dhs.gov

Research Data Repository

The Research Data Repository Project is the only freely available, legally collected repository of large-scale datasets containing real network and system traffic. With the goal of providing a streamlined legal framework to centralize a controlled distribution of datasets while protecting researchers, data providers, and data hosts, the project will accelerate the design, production, and evaluation of next-generation cybersecurity solutions, including commercial products. Today, technology developers and evaluators often determine the efficacy of their technical solutions on the basis of anecdotal evidence or small-scale test experiments. Once created, these data sources will be more widely available and determinations will be based on more comprehensive real-world data.

The project was conceived as a distributed repository with three key components: data providers, data hosts, and a Coordinating Center (CC). Data providers legally supply the data to be shared through the repository; data hosts provide the infrastructure to store the repository data and transfer it to authorized recipients; and the CC provides a centralized mechanism for cataloging available data while managing the submission and review of data requests. The goal of the distributed structure is to provide secure, centralized access to multiple sources of data and promote data sharing while protecting the privacy of the data producers and the security of their networks and data. A Web portal, www.predict.org, provides both public and restricted access to the repository.

In FY 2012, the Research Data Repository was entering a new phase. A highlight of the next step in the project will be the revamping of the legal framework supporting the distribution of the datasets and the addition of new types of dataset collections. In support of this new phase, in FY 2011, the repository's legal structure was updated to be more flexible by providing a mechanism to address classes of datasets covered in the legal agreements, as opposed to specific enumeration of data, and agreement modification for any new data.

FY 2011 Highlights

- New customers and partners were added to the project, including 26 from academia, 24 from commercial industry, 1 foreign and 1 government partner, and 4 non-profit organizations.
- 40 new datasets, comprising approximately 50 terabytes (TB) of information, were added to the repository. The 50 TB of new data represents a 25 percent increase in the amount of data available for experiments, bringing the total amount of available data to more than 250 TB.
- The cybersecurity research community requested 155 accounts and 229 datasets for experiments.

Project Performers

- Packet Clearing House (PCH)
- University of Southern California (USC)
- University of California, San Diego (UCSD)
- Research Triangle Institute (RTI)
- University of Michigan
- Merit Network, Inc.
- Georgia Institute of Technology
- University of Wisconsin
- Global Cyber Risk, LLC

Websites

www.predict.org

Program Manager

Dr. Douglas Maughan, douglas.maughan@hq.dhs.gov

TRUSTWORTHY CYBER INFRASTRUCTURE

About This Program

The Trustworthy Cyber Infrastructure (TCI) program focuses on ensuring that the nati such as the oil and gas pipelines, the information infrastructure, and the Internet, be less vulnerable to malicious and natural events. This program engages industry, gov and academia to improve the core functions of the Internet and critical-sector inform protect their owners, operators, and users, including U.S. government networks and

The Internet connects all other networks, including our nation's critical infrastructure nervous system for our government, our citizens, and our industries. When it is attac far and wide. The Internet's address system, created in 1983, was not built with sec not meant for services that require strict verification of users' identities —such as e envisioned how vast the Internet would become.

The majority of government communications utilize private-sector networks, including critical infrastructures, such as information technology networks, communications networks, financial services networks, the electrical grid, and oil and gas systems. These networks have critical interdependencies, so a failure in one network (for example, the electrical grid) can impact the others (for example, financial networks).

In FY 2011, S&T carried out the Trustworthy Cyber Infrastructure program through three project(s):

- ***Secure Protocols*** — S&T led efforts to forge ahead in developing security protocols for the existing Internet infrastructure (essential to daily Internet operations) so that users are not redirected to unsafe websites or pathways by malicious actors.
- ***Internet Measurement and Attack Modeling*** — In order to improve the protection and defense of critical Internet infrastructure, those critical Internet resources vulnerable to attack must be identified. S&T worked to develop capabilities to map Internet hosts, routers, and modeling and analysis to predict the effects of cyber attacks on commercial and federal infrastructures.
- ***Process Control Systems (PCS) Security*** — S&T led efforts to secure the information systems that control the country's critical infrastructure, including the electrical grid, oil and gas refineries, pipelines, and the financial sector, to reduce vulnerabilities as legacy, standalone systems are networked and brought online.

Secure Protocols

The President's National Strategy to Secure Cyberspace (2003) clearly states the need to "secure the mechanisms of the Internet by improving protocols and routing."

The Internet is made up of three key pieces: the Domain Name System (DNS), Internet Protocol (IP) Addressing, and the routing infrastructure. The DNS maps IP addresses consisting of long sets of numbers to a recognizable set of letters, words, or numbers; the average Internet user recognizes these as Web addresses. IP addresses serve as unique identifiers critical to the construction of networks and the identification of destinations on the Internet. The routing infrastructure relies on the Border Gateway Protocol (BGP) to discover routes between the large networks that make up the Internet.

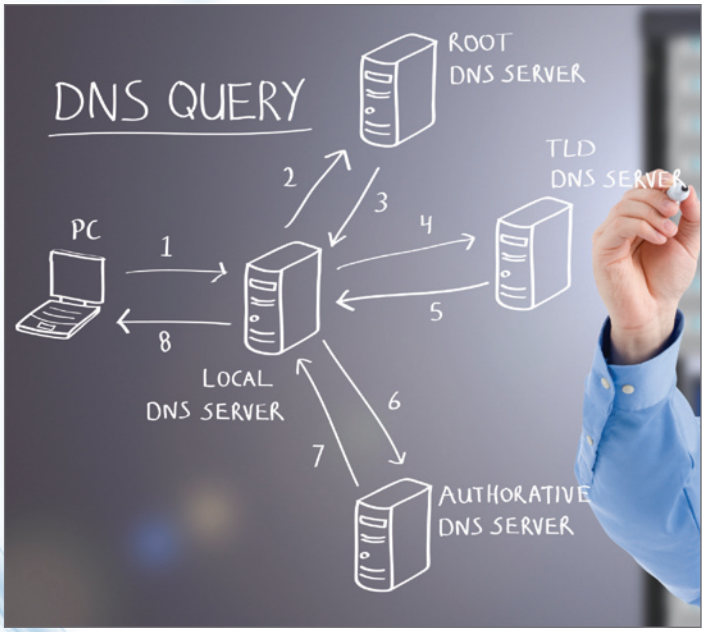
The Secure Protocols Project, established in 2004, aims to solve the lack of secure mechanisms in BGP, DNS, and IP Addressing by securing the endpoints with public/private keys and protecting the path for the communications to eliminate tampering. These are complex, globally distributed systems, owned 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 individual responsibility, it is critical to involve these entities in every step of the process, including the research, development, testing, evaluation, and transition activities necessary to design, implement, standardize, and deploy secure solutions for BGP and DNS.

In order to achieve its goals, the Secure Protocols project is divided into two distinct, yet interrelated initiatives: **Domain Name System Security Extensions (DNSSEC) Deployment Initiative** and **Secure Protocols for the Routing Infrastructure (SPRI)**.

Domain Name System Security Extensions (DNSSEC) Deployment Initiative

The Domain Name System (DNS) is a critical piece of Internet infrastructure that serves as the Internet's "phonebook" by translating human-readable host names into Internet Protocol (IP) addresses. The security, trust, and continued functioning 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. For more than seven years, S&T, in partnership with the National Institute of Standards and Technology (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 organizations in the public and private sectors.

In FY 2011, a major focus of the initiative was the further development and distribution of tools, both to help end users deploy and configure DNSSEC and to better monitor the deployment of DNSSEC. Going forward, S&T will focus more attention on the deployment initiative's development of tools that will make it easier for operators to incorporate DNSSEC into their domains, allow end users to trust that the data they are accessing is valid, and better monitor the impact of the deployment of DNSSEC.



FY 2011 Highlights

- S&T efforts contributed to more than 30 percent of all top-level domains that are currently digitally signed with certificates, including .com, .gov, .uk, and .org.
- S&T received a National Cybersecurity Innovation Award at the Sans Institute's Second Annual National Cybersecurity Innovation Conference for its DNSSEC Deployment Initiative.
- The DNSSEC Tools were extended to provide visualization of various aspects of DNSSEC, such as user applications and network operator troubleshooting. When used in conjunction with the DNSSEC validating browser, this visualization provides the means of showing users which DNS names that they are browsing have been validated — and which have not.
- NIST joined its .gov DNSSEC deployment monitoring tool with its .gov IPv6 deployment monitoring tool to show a unified view of the deployment efforts of DNSSEC and IPv6 in the .gov domain.
- S&T continued communications with major Top Level Domains (TLDs) and Country Code TLDs (ccTLDs) to facilitate and coordinate the rollout of DNSSEC in key, infrastructure-level zones.

Project Performers

- Shinkuro, Inc.
- Sparta, Inc., a Parsons Company
- National Institute of Standards and Technology (NIST)

Websites

www.dnssec-deployment.org
www.dnssec-tools.org

Program Manager

Edward Rhyne, edward.rhyne@st.dhs.gov

Secure Protocols for the Routing Infrastructure (SPRI)

In 2004, to improve the security of Internet Addressing and Routing by making them less susceptible to disruption and misdirection caused maliciously or through misconfiguration, DHS S&T started the Secure Protocols for the Routing Infrastructure effort. IP (Internet Protocol) addresses serve as unique identifiers, critical to the construction of networks and identification of destinations. The Resource Public Key Infrastructure (RPKI) standard, developed in partnership with the Internet community, provides a method for verifying the authenticity of IP addresses. The routing infrastructure relies on the Border Gateway Protocol (BGP) to discover routes between the large networks that make up the Internet. Currently, it is challenging to determine if a BGP route has been altered, allowing for the interception or misdirection of traffic. The BGP Security (BGPSEC) standard allows for the detection of changes to the routing path, while taking into consideration the scale and complexity of global Internet routing. DHS S&T has played a leading role in the development of both standards and in promoting their adoption.

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, S&T is developing tools to help 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 2011 Highlights

- The initial nine draft standard documents for BGPSEC were submitted to the Internet Engineering Task Force (IETF), beginning the adoption process. The documents were developed by a DHS S&T-led design team made up of routing manufacturers, network operators, content providers, government researchers, and academics.
- All five of the Regional Internet Registries (RIRs), organizations responsible for distributing Internet addresses, publically deployed RPKI systems that can issue address certificates. Four of the registries completed piloting and made these systems operationally available. The final registry is predicted to have the system operationally available by the end of 2012.

Project Performers

- Sparta, Inc., a Parsons Company
- Raytheon BBN Technologies

Website

www.cyber.st.dhs.gov/spri

Program Manager

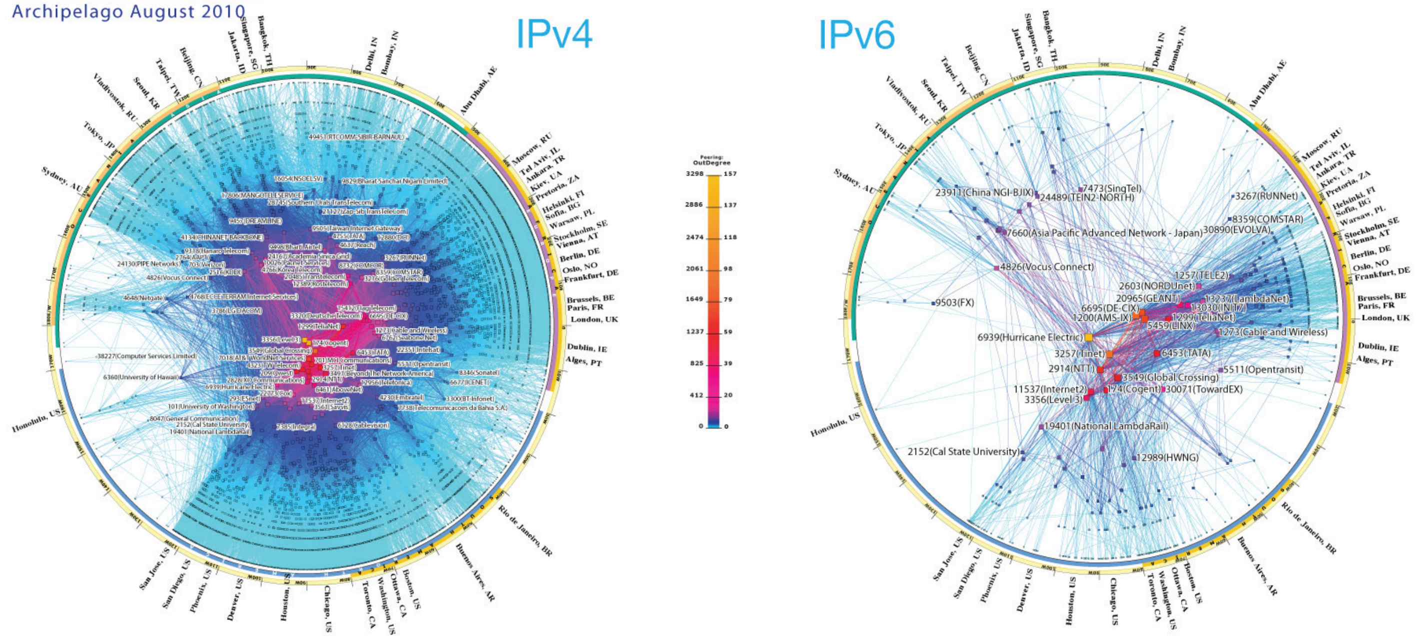
Luke Berndt, luke.berndt@hq.dhs.gov

Internet Measurement and Attack Modeling (IMAM)

The protection of cyber infrastructure depends on the ability to identify critical Internet resources that are subject to attack. S&T's Internet Measurement and Attack Modeling (IMAM) project is focused on the development and application of modeling and analysis capabilities to predict the effects of cyber attacks on federal government installations and other critical infrastructure. It does this through the detection of malware and botnets, situational understanding, and attack attribution. The technologies being developed are critical to U.S. national security missions — in particular, to missions that support DHS watch-center operations and conduct analyses of cyber infrastructure threats and risks, missions that strengthen U.S. military, and civilian communications environments that rely on the Internet.

In FY 2011, IMAM made considerable progress. A powerful and versatile globally distributed measurement infrastructure, Archipelago (Ark), consisting of 56 monitors, was deployed in 30 countries on 6 continents. There are two different versions of IP (Internet Protocol), IPv4 and IPv6. IPv6 is an evolutionary upgrade to the IP; the two versions will coexist. IPv4 is a 32-bit numeric address written in decimal, using the format 1.2.3.4. IPv6 is a 128-bit address written in hexadecimal, using short digital strings separated by colons. Ark is now continuously gathering the largest set of IPv4 and IPv6 topology data made available to academic researchers and government agencies. In addition, completed versions of the Correlation Layers for Information Query and Exploration (CLIQUE) and the Traffic Circle cyber visualization tools were released, helping analysts identify malicious activity in high-volume computer network data through behavior modeling coupled with interactive visual analysis. Furthermore, the latest version of the real-time Border Gateway Protocol data collection tool (BGPmon) was released — a major upgrade to previous versions of this open-source software, incorporating several user-requested features as well as optimizations and bug fixes that accompany any updated version. By providing BGP data in real time, including data from Oregon RouteViews, BGPmon allows real-time detection of routing hijacks and other routing events.

CAIDA's IPv4 & IPv6 AS Core
AS-level INTERNET GRAPH
Archipelago August 2010



FY 2011 Highlights

- S&T funded development of monitors and conducted continuous probing of BGP-announced IPv6 prefixes to map and better understand trends in the IPv6 Internet space.
- S&T provided support to the United States Computer Emergency Readiness Team (US-CERT) in developing specifications for and testing its new Enhanced Analytic Database capability.
- S&T-funded development of a new approach to discover anycast (used by most large DNS services), to detect masquerading, such as “man-in-the-middle” attacks.
- Data from the DHS-supported Oregon RouteViews project continued to be one of the most cited resources for Internet routing research and operations. Data was cited at the top computer science networking conferences, such as the conference of the Association for Computing Machinery’s Special Interest Group on Data Communication (ACM SIGCOMM) and the IEEE Conference on Computer Communications (INFOCOM).

Project Performers

- University of Southern California, Internet Sciences Institute (USC-ISI)
- University of California at San Diego (UCSD)
- Pacific Northwest National Laboratory (PNNL)
- Colorado State University (CSU)

Websites

USC-ISI: www.isi.edu/ant/address/browse
UCSD: www.caida.org/projects/cybersecurity
CSU: www.routeviews.org, bgpmon.netsec.colostate.edu

Program Manager

Edward Rhyne, edward.rhyne@st.dhs.gov

asia-pacific
disa
MULTICAST
RESERVED
asia-pacific
asia - pacific
asia-pacific
us-dod
north america
europe
north america
asia-
pacific
various
registrars
europe
north america
north america
europe
north america
asia-pacific
various
europe
north america
africa
registrars
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Responses: postive: green, negative: red, mix: yellow

LANDER Map of Internet Address Space Use. (C) 2007-2011 USC/Information Sciences Institute. www.isi.edu/ant/address
visualization: John Heidemann from layout suggested by Randall Munroe; probing: Yuri Pradkin;
methodology: John Heidemann, Yuri Pryadkin, Ramesh Govindan, Christos Papadopoulos, Joseph Bannister.
Dataset USC/LANDER-internet_address_census_it44c-20111102, taken November 2011.
Data shows the results of pings of about 3 billion IP addresses, with color indicating the reply.
Blue hatched: unallocated, cyan hatched: reserved

Process Control System Security

Process Control Systems (PCSs) are computer-based facilities, systems, and equipment used to remotely monitor and control sensitive processes and physical functions. They are responsible for the distributed monitoring and control of many of the nation's critical infrastructures, such as the electrical power grid and oil and gas refineries and pipelines. As these traditionally stand-alone systems are being connected and brought online, vulnerabilities have been introduced with the migration to standard IT components, introduction of standard networking technology such as TCP/IP, and integration of business and process control networks.

These new vulnerabilities have increased the need for cybersecurity in PCSs, particularly in the energy sector. Critical to national interest, the electric power grid underlies virtually all economic activity and essential government services. Since the majority of the critical infrastructure is not owned by the federal government, but rather by private companies that are often reluctant to share information due to their wish to maintain competitive advantages, it is up to the federal government to fund research and development and provide transition pathways for the vendor community to assist infrastructure owners.

To address these needs, the PCS Security Project was established in 2009. Requirements for the project come from the Cyber Security Requirements Gathering Process, internal to S&T, as well as from industry sources, including the Industrial Control Systems Joint Working Group (ICSJWG), led by the DHS National Protection and Programs Directorate (NPPD), and the Department of Energy (DOE) Roadmap to Secure Control Systems in the Energy Sector.

In order to focus on the most critical areas, the PCS Security Project is broken into two separate efforts: **Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC)** and **Trustworthy Cyber Infrastructure for the Power Grid (TCIP-G)**.

Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC)

In 2004, DHS identified the oil and gas industry's process control systems and supervisory control and data acquisition (SCADA) systems as potential points of threat from terrorists seeking to destabilize the energy industry supply capabilities and the U.S. economy. Recognizing this vulnerability, industry and government came together to start the LOGIIC consortium, an ongoing collaboration between oil and natural gas companies and S&T.

The LOGIIC consortium facilitates cooperative research, development, testing, and evaluation procedures 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. The objective of LOGIIC is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality.

LOGIIC represents a model partnership between government and industry. In this effort, the oil and gas companies contributed the operational environment, expertise, and project management; the vendor companies provided security expertise and products; and S&T contributed testing facilities and independent research staff with technical security expertise. Current members of LOGIIC include: BP, Chevron, Shell, Total, and other large oil and gas companies that operate significant global energy infrastructure.

FY 2011 Highlights

- The LOGIIC consortium completed the Safety Instrumented Systems (SIS) Project. Vendors used the findings from their specific evaluations to mitigate vulnerabilities in their products. The changes will benefit all the owners and operators that use their products. The International Society of Automation (ISA), a major standards body, offered to use the work from this project to incorporate into one or more major cybersecurity standards for process control systems.
- The LOGIIC consortium completed the comparison of four of the world's largest oil and gas companies' cybersecurity standards, to look for areas of common interest and gaps. The oil and gas companies are using the results to update their standards.
- LOGIIC members approved communications guidelines that allow many LOGIIC project results to be shared with the public, and permit greater information sharing about the consortium and the value of the public/private partnership model.

Project Performers

- SRI International

Website

www.logiic.org

Program Manager

Greg Wigton, gregory.wigton@hq.dhs.gov

Trustworthy Cyber Infrastructure for the Power Grid (TCIP-G)

S&T and DOE jointly funded the Trustworthy Cyber Infrastructure for the Power Grid (TCIP-G) effort to address the challenge of protecting the nation's power grid by significantly improving the way the power grid infrastructure is built, thus making it more secure, reliable, and safe.

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 from both malicious cyber attacks and accidental failures. 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.

TCIP-G's research focuses on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber attacks, 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. 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.

In the past year, the project made considerable progress in developing more secure technologies and raising awareness across multiple areas, including Advanced Metering Infrastructure (AMI), which is an important component of the Smart Grid, enabling demand response, time-of-use pricing and timely outage detection; standards in Home Area Networks (HAN) and integration with AMI; educational efforts to increase knowledge of power grid technologies among students ranging from elementary to graduate levels; and supervisory control and data acquisition (SCADA) network access and communication with Internet protocols.

FY 2011 Highlights

- The TCIP-G Center developed a prototype detection module for AMI networks. The module uses conventional signature-based detection with a specification-based approach, which has the potential to defend against previously unknown attacks, known as zero-day exploits against AMI networks.
- The TCIP-G Center co-developed the Network Access Policy Tool (NetAPT), which assists in identifying the routable paths possible between critical networks and nodes. NetAPT matured to the point that it is in evaluation for pilot deployment at a major utility, a rural electric cooperative, and at theSERC Reliability Corporation.
- The TCIP-G Center identified vulnerabilities in ZigBee, the wireless communication protocol used for HAN. The TCIP-G team submitted reports for migration with respective vendors.
- The TCIP-G Center held a summer school program that focused on information trust for grid systems for graduate students and professional practitioners, and developed multimedia curriculum material on the smart grid, geared toward elementary and high school students.

Project Performers

- University of Illinois at Urbana-Champaign (UIUC)

Website

www.tcipg.org

Program Manager

Greg Wigton, gregory.wigton@hq.dhs.gov

FOUNDATIONAL ELEMENTS OF CYBER SYSTEMS

About This Program

The only long-term solution to the vulnerabilities of today's networking and information technologies is to ensure that future generations of these technologies are designed with security built in from the ground up. The Foundational Elements of Cyber Systems (FECS) Program focuses R&D activities on the characteristics essential to the desired end states of trustworthy cyber systems. A system needs to have sound security requirements, and users need strong assurance that the system meets those requirements. The FECS program will accelerate the transition of new cybersecurity technologies into commercial products and services. End users of these technologies include first responders, critical infrastructure providers, the banking and finance sector, private industry, and government.

In FY 2011, S&T carried out the FECS program through several projects, two of which had noteworthy accomplishments this year:

- ***Homeland Open Security Technology (HOST)*** — S&T is a driving force behind evaluating and promoting open security methods, models, and technologies, and identifying viable and sustainable approaches that support national cybersecurity objectives. Through HOST, S&T led efforts of discovery, collaboration, and development in open-source software and practices that produce a measurable impact.
- ***Software Quality Assurance*** — S&T worked to develop tools, techniques, and environments to analyze software, address the presence of internal flaws and vulnerabilities in software, and improve software security associated with critical infrastructure (energy, transportation, telecommunications, banking and finance, and other infrastructure types).

Homeland Open Security Technologies (HOST)

Open-source software, composed of source code that is available for use, modification, and redistribution, provides many innovative security solutions that are not being successfully leveraged by government. The shared nature of open source means that improvements made by one agency benefit the larger community, yet government acquisition and security certification can make it challenging to use these solutions. The Homeland Open Security Technologies (HOST) project focuses on improving awareness of open-source security solutions available to all levels of government, inventorying those that have been successfully deployed, and sponsoring development in areas where security solutions do not currently exist.

HOST is engaging thought leaders from the open-source and open-government community. An initial group of government users of open-source software, including users from NASA, DoD, the DHS National Protection and Programs Directorate, the Chief Information Officer, and Immigration and Customs Enforcement, came together to form an executive committee for this project. The Executive Committee will help identify transition partners for technologies they prioritize for development.

Initial sponsorship focused on developing the first open-source, multithreaded intrusion-detection system, called Suricata, and supporting the Federal Information Processing Standards validation of OpenSSL, an open-source encryption library used in both open source and commercial software. OpenSSL is one of the most popular encryption libraries and is used in a variety of Web browsers and email applications.

FY 2011 Highlights

- The formation and initial meeting of the HOST Executive Committee provided guidance for upcoming investments.
- Suricata was integrated into commercial products from three vendors and is being used on government networks.

Project Performers

- Georgia Tech Research Institute (GTRI)
- Open Source Software Institute
- Open Information Security Foundation

Website

www.opencybersecurity.org

Program Manager

Luke Berndt, *luke.berndt@hq.dhs.gov*

Software Quality Assurance (SQA)

Vulnerabilities in software are arguably the weakest link in the cybersecurity chain. To help change this, tools, technologies and techniques are being developed to analyze software, address the presence of internal flaws and vulnerabilities in software, and improve software security associated with critical infrastructure (energy, transportation, telecommunications, banking and finance, and other sectors).

Through CSD's Cyber Security Research and Development Broad Agency Announcement 11-02, and the S&T Small Business Innovation Research (SBIR) program, solutions will soon be underway to improve the quality and reliability of software. These solutions will include capabilities to

- extend static analysis techniques for source and object codes to allow them to systematically explore the platform space. This will involve utilizing distributed build-and-test systems to harness the cloud, with centralized collation and presentation of analysis results. Existing technology transition channels will be leveraged to achieve maximum impact on industry and government;
- provide a flexible interface to ingest the results of a wide array of vulnerability tools, enhance existing and create additional visualizations, and increase the level of integration with software development life cycle (SDLC) tools; and
- produce an open-source implementation of the framework for unified and consistent reporting of vulnerabilities. This implementation will include a ready-to-use open-source composite vulnerability analyzer that integrates five existing open-source vulnerability-detection tools, a protocol for exchanging vulnerability findings, blueprints for adaptors of the framework, and practical usability and accuracy data based on a case study.

FY 2011 Highlights

- S&T-funded experiments demonstrated that the analysis of software as configured for a single platform may fail to detect between 25 and 40 percent of the underlying defects.
- S&T conducted user interviews and defined workflow, use cases, requirements, and wireframes that are helping to guide the development of the Software Assurance Visual Analytic Tool. A first prototype is expected in early 2012.
- S&T supported the development of www.cwevis.org, a reference website to visualize Common Weakness Enumeration (CWE) in the source code.

Project Performers

- GrammaTech
- Applied Visions
- Data Access Technologies

Program Manager

Edward Rhyne, edward.rhyne@st.dhs.gov

CYBERSECURITY USER PROTECTION & EDUCATION

About This Program

People are users of systems and infrastructures. They may be everyday citizens usin, various tasks, they may be cybersecurity professionals, or they may be cyber crimina activity. The Cybersecurity User Protection & Education (CUPE) program focuses R&I types of users — improving the security and protection of user online activity, attracti cybersecurity warriors, and providing the tools needed for investigating cyber-crimina

In FY 2011, S&T carried out the CUPE program through three projects:

- ***Cyber Security Competitions*** — S&T supported cybersecurity competitions, which shortage of technically skilled people required to operate and support deployed sy educating young individuals who can design secure systems and create sophistica malicious acts. Supported competitions included the National Collegiate Cyber De and the U.S. Cyber Challenge (USCC), both conducted in support of the National Ir Education (NICE).
- ***Cyber Security Forensics*** — S&T worked to develop new cyber forensic analysis to techniques for law enforcement officers and forensic examiners to address the full ra
- ***Identity Management and Data Privacy Technologies*** — S&T made strides toward e information-sharing environments and the protection of users by improving authenti devices, and software applications across all levels of government. The Identity Ma Technologies project addresses the inadequate number of security, trust, usability, that currently exist to secure interactions among stakeholders who wish to ensure tl protected and managed.

Cyber Security Competitions

Cybersecurity competitions help 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 focus on alleviating the shortage of technically skilled people required to operate and support systems already deployed but also on educating young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts.

In FY 2011, S&T provided funding to support the development and execution of the Collegiate Cyber Defense Competition (CCDC) and the U.S. Cyber Challenge (USCC). Registration for USCC Cyber Foundations included 26 states and almost 1,000 students. USCC also conducted six summer cyber camps in Maryland, California, Delaware, Virginia, and Missouri, with participation of 210 students in total. Each camp featured four days of intense instruction, culminating in a Capture the Flag competition. Over 1,300 students from 109 colleges and universities participated in CCDC events this year. CCDC was recognized for its efforts to promote a cybersecurity curriculum in institutions of higher learning by the 111th Congress (H. Res 1244) and was mentioned as a model program in the White House's 2009 Cyberspace Policy Review. This year, the CCDC program was also honored with the Visa Leadership in Security Award.

FY 2011 Highlights

- USCC more-than doubled student participation in the Cyber Foundations high school competition, with more than 2,000 students registered in the Fall 2011 competition.
- USCC conducted six cyber camps with more than 200 students through the summer and fall.
- A virtual regional event was launched to allow schools in remote locations participate in the CCDC program — for example, schools in Alaska or Hawaii.
- 109 schools participated in CCDC events, making it the largest collegiate cyber defense competition program in the nation.

Project Performers

- Center for Internet Security (CIS)
- University of Texas at San Antonio (UTSA)

Websites

workforce.cisecurity.org
www.nationalccdc.org

Program Manager

Edward Rhyne, edward.rhyne@st.dhs.gov

Cyber Security Forensics

The role of computers and portable media devices (for example, cell phones, GPS devices) in criminal and terrorist activity has increased significantly in recent years. Law enforcement officers and forensic examiners face a constant challenge to stay ahead of the latest technologies as their roles become more significant in criminal and terrorist investigations. In response to this challenge, CSD, working with DHS components, including U.S. Secret Service (USSS), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and the Federal Law Enforcement Training Center (FLETC), and other federal, state and municipal law enforcement agencies, initiated the Cyber Security Forensics project in 2009.

The Cyber Security Forensics project is developing new cyber forensic analysis tools and investigative techniques for law-enforcement officers and forensic examiners to address the full range of cyber-related crimes. Additionally, the CSD-sponsored Cyber Forensics Working Group (CFWG) 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.

A particularly important subset of cyber forensics, identified as a result of discussions held during CFWG meetings, is the analysis of portable media devices such as "thumb drives," iPods, and phones. The small size and versatility of portable media devices make them useful tools in the conduct of criminal and terrorist activity. Law enforcement officers require tools that can recover system files, operating system information, applications, deleted files, and unallocated space from portable digital media storage devices.

During FY 2011, the Cyber Security Forensics project funded work with the University of Tulsa (TU) regarding gaining physical access to, imaging, and mounting/parsing extractions of mobile phones. The USSS, which maintains an embedded-device forensics laboratory on the TU campus, worked hand-in-hand with students who participate in the National Science Foundation-funded TU Cyber Corps Program. S&T's funding supported Cyber Corps students who are pursuing advanced degrees in Computer Science or Electrical Engineering. This project created a significant capability for all of law enforcement in this new and dynamic technological area.

Also in the area of portable-media examination tools, in FY 2011, the Cyber Security Forensics project focused on the development of a unified tool set specifically designed to examine GPS devices in a manner consistent with the best practices of handling digital media. Logical analysis of GPS devices is often a very labor-intensive process for law-enforcement labs, and few tools are available for use by first responders in the field. Labs are also often constrained by a reliance on technologies developed by GPS vendors that are only compatible with those vendors' products. The device developed in this project will be a single platform that is manufacturer-agnostic, and will have the inherent functionality to support operators in the field, forensic examiners in a lab, and intelligence analysts seeking to identify patterns and reveal trends.

Another area of focus for the Cyber Security Forensics project in FY 2011 was starting the development of a secure, web-based forum for collaboration and dissemination of information, tools, and technologies for cyber forensics practitioners. When completed, the CyberForensics Electronic Technology ClearingHouse (CyberFETCH) will be a resource available to practitioners, investigators, analysts, and technologists to encourage information sharing across agencies, especially as the number of cyber crimes increases. Examples of the types of information envisioned for the site include forensic tool testing reports and information regarding ongoing research efforts across the community.

FY 2011 Highlights

- S&T funded the release of the first prototype of the First Responder Cyber Field Kit to 20 federal, state, and local agencies for a 6-month test period.
- The assessment architecture developed through S&T funding to test the vulnerabilities of the open-source Wireshark network monitoring tool gained outside interest and will be utilized by Google to test its Chrome Internet browser.
- S&T funded work to gather detailed information on more than 80 insider-threat cases, in collaboration with the USSS, contributing to a comprehensive view of how incidents negatively affected different financial institutions.
- S&T funded the National Institute of Standards and Technology's (NIST) National Software Reference Library, which published four quarterly releases, growing by 10 million records.

Project Performers

- ADF Solutions, Inc.
- Berla Corporation
- Carnegie Mellon University
- ITT Exelis
- NIST
- Purdue University
- University of Tulsa
- University of Wisconsin

Program Manager

Dr. Douglas Maughan, douglas.maughan@hq.dhs.gov

Identity Management and Data Privacy Technologies

The 2009 White House Cyberspace Policy Review outlines a way forward in building a reliable, resilient, trustworthy digital infrastructure for the future. One of the top 10 near-term action items discusses building "a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation."

The President and Congress directed DHS to prevent and protect against terrorist attacks and respond to both man-made and natural disasters. To do this, DHS needs to share information across multiple domains and jurisdictions in a secure manner. Agencies and organizations are experiencing a lack of infrastructure and technologies to share and coordinate information effectively, not because of inadequate quantities of data and information-sharing environments, but because of an inadequate amount of security, trust, usability, policies, and procedures.

In order to achieve its goals, the Identity Management and Data Privacy Technologies project is divided into two distinct, yet interrelated activities: **Identity and Access Management** and **Data Privacy Technologies**.

Identity and Access Management

The identity management lifecycle is a system of procedures, policies and technologies to manage the entitlements of electronic user credentials (for example, username/password, smart card). This lifecycle includes user registration and identity proofing, binding identity with attributes into secure tokens, credential issuance, credential usage, and credential revocation.

From the lifecycle, S&T is conducting research in identity-proofing and "usage" of issued credentials, including using credentials for access to physical and logical systems.

Having established the S&T Identity Management Testbed, S&T is able to mitigate technical risks and explore identity, credentialing, and access-management architectures. This mitigation is achieved by developing proof-of-concept solutions, guiding standards development, conducting pilots, and demonstrating the utility of proposed solutions for the Homeland Security Enterprise.

S&T is researching and developing identity management technologies to enable seamless and secure interactions among federal, state, local, public, and private-sector stakeholders.

Benefits of Identity Management

- Maintains organizational sovereignty
- Eliminates the need for one organization to manage and maintain another's user identities
- Facilitates trust across organizations through the acceptance of one another's identification cards
- Reduces the need for multiple credentials by providing an interoperable solution for accepting cross-domain identification cards

Federal

Within the Identity Management project, S&T is providing research and development solutions affecting all federal agencies by supporting the General Services Administration (GSA) Office of Governmentwide PolicyIdentity Assurance and Trusted Access Division in its role as executive agent of the Identity Credentialing Access Management Subcommittee (ICAMSC). By leveraging the S&T research efforts conducted in the Identity Management Testbed, GSA is able to transition the research into operational requirements and include the developments in documents, such as the Federal, Identity, Credentialing, and Access Management (FICAM) Roadmap.

State and Local Participants

- Colorado
- Maryland
- Virginia
- District of Columbia
- Missouri
- Southwest Texas
- Pennsylvania
- Chester County, PA
- Pittsburgh, PA
- West Virginia
- Hawaii
- Rhode Island
- Illinois

State, Local and Public

In a partnership between S&T and the Federal Emergency Management Agency (FEMA), a working group consisting of state and local agencies as well as fusion centers seeks to increase the adoption of credentials (for example, Personal Identity Verification-Interoperable [PIV-I]/First Responder Authentication Credential [FRAC]) that are able to interoperate across jurisdictional lines for both physical and logical access control. The PIV-I/FRAC Technology Transition Working Group meets quarterly to share lessons learned and success stories, provide policy makers with a unified emergency manager perspective, and identify technology and capability gaps where S&T can provide research, development, and test & evaluation support. S&T is currently laying the groundwork for a pilot, to be finalized in FY 2013, demonstrating the ability for a standards-based transmission of local jurisdiction attributes to be coordinated with FEMA's emergency responder attribute repository in a potential emergency operation.

Private Sector

S&T is supporting an effort with the Financial Services Sector Coordinating Council (FSSCC) to address an identity-proofing requirement to protect citizens and prevent financial loss by enhancing the resilience, security, integrity, and usability of financial services. The effort requires policy evaluation and technical development of architectural approaches and processes for confirming identity credentials presented when opening a bank account. This supports the National Security for Trusted Identities in Cyberspace (NSTIC) goal for individuals and organizations to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services. The NSTIC is directly tracking the S&T effort with the finance sector.

FY 2011 Highlights

- The White House facilitated a Memorandum of Understanding signed by S&T, the National Institute of Standards and Technology, and the FSSCC to accelerate cybersecurity research and development activities for protecting the physical and electronic infrastructures.
- S&T funded the development of interoperable communication standards, protocols, and cybersecurity tools for protecting access to data and resources, including the transition of the Backend Attribute Exchange profile and architecture specification to the Federal Identity, Credentialing, and Access Management Subcommittee, under the Federal CIO.
- S&T collaborated with multiple commercial-off-the-shelf vendors and industry in the web services, security and identity domain, to implement standards and protocols, making products ready and available for integrators.

Project Performers

- Johns Hopkins University, Applied Physics Lab
- Queralt Inc.

Websites

www.cyber.st.dhs.gov/docs/Moving-Towards-Interoperability.pdf
www.ahcusa.org/PIV-I%20TTWG.html

Program Manager

Karyn Higa-Smith, karyn.higa-smith@hq.dhs.gov

Data Privacy Technologies

Privacy-enhancing technology (PET) is the set of technologies and associated business processes that help organizations responsibly manage personal information in a manner that protects individual privacy while complying with applicable law, policy, and mission. PETs are critical enablers of information sharing; they foster confidence that personal information is being used appropriately while minimizing privacy risk.

S&T is supporting the application of privacy technology to Homeland Security Enterprise missions by exploring, refining, and integrating technologies and techniques, and piloting the results. S&T is identifying and prioritizing specific DHS privacy technology needs, which include the use of data anonymization tools and techniques to effectively address those needs. S&T is also collaborating with state and local fusion centers to enhance the understanding of information-sharing mission needs.

To further understand the DHS-specific requirements, S&T convened the Privacy Working Group, composed of privacy stakeholders, including the DHS Privacy Office, Director of Privacy Technologies, and various DHS agency components — Immigration and Customs Enforcement(ICE), U.S. Citizenship and Immigration Services, Customs and Border Protection, US-VISIT, and the Transportation Security Administration — to understand their operational-level view of privacy gaps within DHS. The Privacy Working Group meets annually to gather requirements to address common capability gaps.

FY 2011 Highlights

- S&T funded the development of a methodology to analyze structured data for possible anonymization of personally identifiable information. This methodology received a letter of commendation from the ICE Privacy Office.
- Work funded by S&T was awarded a Best Paper award at the Institute of Electrical and Electronic Engineers (IEEE) Homeland Security Technology (HST) Conference for innovative research in Policy Reasoning Over Cross-Jurisdictional Data Transactions Occurring in a Decentralized Environment.

Project Performers

- MITRE Homeland Security Systems Engineering Development Institute (HS SEDI)
- Massachusetts Institute of Technology

Program Manager

Karyn Higa-Smith, *karyn.higa-smith@hq.dhs.gov*

CYBERSECURITY TECHNOLOGY EVALUATION & TRANSITION

About This Program

To ensure the effective deployment and operational use of new cybersecurity innovations, the “valley of death” chasm must be bridged by technology transition through cooperative efforts and investments by both the research and acquisition communities. The Cyber Technology Evaluation and Transition (CTET) program provides a coordinated process of assessments, evaluations, and operational experiments and pilots in order to transition the fruits of research into practice.

The assessment and evaluation of cybersecurity technologies developed both inside and outside of S&T are critical prior to operational deployment within the Homeland Security Enterprise. This stage includes Red Team evaluations to identify vulnerabilities and weaknesses, as well as operational assessments. Experience shows that transition plans developed and applied early in the lifecycle of the research program, if accompanied by probable transition paths for the research product, are effective in achieving successful transfer from research to application and use. These transition paths are affected by the nature of the technology, the intended end user, participants in the research program, and other external circumstances.

In FY 2011, S&T carried out the CTET program carried out its activities through three projects:

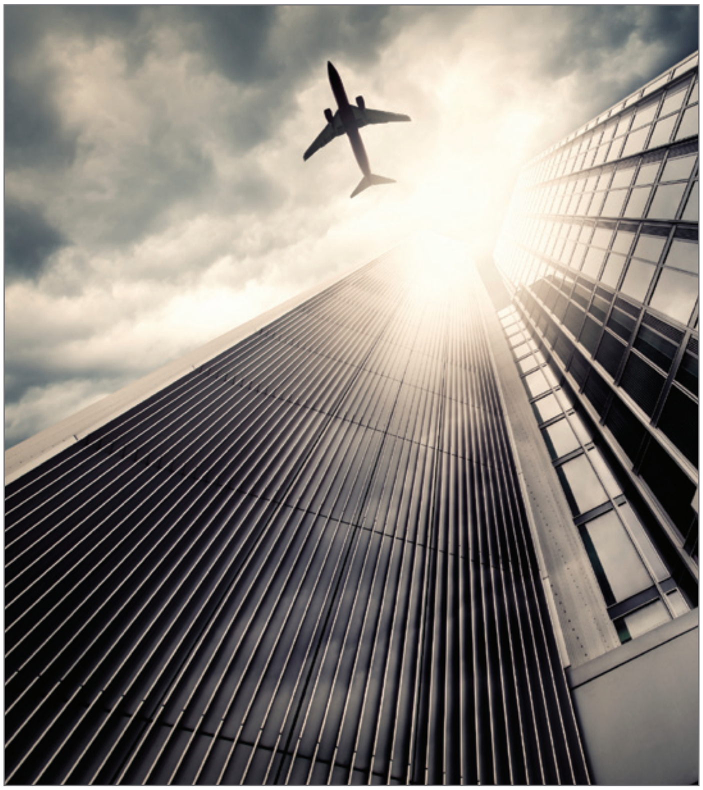
- ***Cyber Security Experiments and Pilots*** — Through experiments and pilots, S&T developed cybersecurity technologies that were tested and evaluated in operational environments so that solutions could move from the lab to real life, securing the networks of users who need them.
- ***Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE)*** — S&T led efforts to enable private-sector entities located within critical infrastructures to conduct collaborative, realistic, fully immersive, scenario-based exercises with response decisions made by enterprise risk managers.
- ***Cyber Security Assessments and Evaluations*** — To increase overall system security and transition of cybersecurity solutions into commercial products, S&T addressed component and system vulnerabilities throughout the development lifecycle, from design to operational evaluation, and facilitated the dialogue between researchers, technology entrepreneurs, and large companies.

Cyber Security Experiments and Pilots

The Cyber Security Experiments and Pilots project addresses cybersecurity requirements from DHS components and critical infrastructure users in support of operational missions in critical infrastructure protection. Experiments and pilots allow technologies developed at S&T to be tested and evaluated in operational environments while allowing S&T to provide feedback to performers and vendors. This feedback, in turn, allows DHS components to refine their requirements and ultimately make their infrastructure more secure.

In FY 2011, while working with its Office of the Chief Information Officer, S&T, completed the Department of Homeland Security's Secure Wireless Access Pilot (DSWAP) experiment with the Federal Law Enforcement Training Center (FLETC).

DSWAP demonstrates a method to securely connect computers, tablets, and smartphones to DHS networks by using public wireless infrastructure. The technology incorporates multiple security components, including screen privacy filters, encrypted hard drives, traffic monitoring software, firewall and anti-virus protection, and wireless policy managers. This technology will ensure the secure delivery of critical information via wireless technologies. The lessons learned from this pilot will enable FLETC and DHS S&T CIOs to identify vulnerabilities in current wireless policy and make recommendations for future changes to their infrastructure.



FY 2011 Highlights

- S&T completed the DSWAP with FLETC to allow users to access the DHS network securely through public WIFI networks

Program Manager

Greg Wigton, *gregory.wigton@hq.dhs.gov*

Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE)

A critical area of focus for DHS is the development and deployment of technologies used to protect the nation's cyber infrastructure, including the Internet and other critical infrastructures that depend on computer systems for their mission. Regulators, business continuity planners, and enterprise risk managers within the banking and finance sector rely on computer systems and have a priority need for a computer-based capability to examine a variety of risk scenarios. Scenarios include the intentional and unintentional destruction or disruption of physical and cyber infrastructure affecting key business processes. Given the current threat environment, this is an urgent need demanding immediate attention.

S&T initiated the Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE) Project in November 2008, in coordination with the Financial Services Sector Coordinating Council's Research and Development Committee. The goal of DECIDE is to allow enterprise decision makers to evaluate responses to operational disruptions of market-based transactions across networks; provide a dedicated exercise capability for several critical infrastructures in the U.S.; and foster an effective, practiced business continuity effort to deal with increasingly sophisticated cyber threats.

DECIDE will enable private-sector entities located within critical infrastructures to conduct collaborative, realistic, fully-immersive, scenario-based exercises with response decisions made by enterprise risk managers. These exercises will be based on realistic impacts to individual business models. It will reduce the time and cost of building large-scale distributed exercises, ensure businesses a return on investment for participating in such exercises, and address the problem of sharing business-sensitive information with competitors and regulators. Ultimately, the project will allow more businesses to realistically exercise contingency plans.

FY 2011 Highlights

- Three alpha release versions (0.6, 0.7, and 0.8) of DECIDE were completed, each developed, tested, and delivered with full functionality. The DECIDE-FS tool developed from a simple simulation to a robust game environment that encourages players to make difficult "profit vs. security" decisions.
- All technical and exercise design requirements needed to create a complex exercise distributed between New York, Chicago, and Washington, D.C. were met, culminating in a successful dry run.

Project Performers

- Norwich University Applied Research Institutes

Program Manager

Greg Wigton, gregory.wigton@hq.dhs.gov

Cyber Security Assessment and Evaluation

While traditional research and development of cybersecurity technologies is important, ensuring that those same technologies are appropriately evaluated prior to operational deployment within the Homeland Security Enterprise is equally important. In response to this need, S&T established the Cyber Security Assessment and Evaluation project to gauge whether technologies developed both within and outside of S&T are useful for and ready to be deployed to the Homeland Security Enterprise by performing activities such as Red Team evaluations to identify vulnerabilities and weaknesses.

The solutions proposed by these activities support the entire cybersecurity community, both within the federal government and in the private sector, in identifying and assessing cyber threats and vulnerabilities and assisting in the acquisition, evaluation, and deployment of cybersecurity technologies.

Within S&T, CSD-supported project performers execute a technology transition process whereby their tools and technologies can be acquired, evaluated, and transitioned to appropriate end users; these end users include owners and operators of U.S. critical infrastructures, private-sector entities, and federal, state, and local law-enforcement agencies. By leveraging the cutting-edge tools and technologies being developed specifically to address cybersecurity needs, end users have the opportunity to identify contemporary threats and enhance their security posture.

In FY 2011, three deployments of DHS-funded technology, numerous technology evaluations, and two technology transition forums were held, both to showcase the cybersecurity technologies and solutions developed by S&T-funded researchers and to expose other federal agencies and large system integrators and users to the transitionable technologies.

FY 2011 Highlights

- A deployment of Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks (CAULDRON) to a federal law enforcement agency took place. CAULDRON is a risk assessment application that searches for sequences of interdependent vulnerabilities distributed across a network.
- VIAssist was deployed to the forensic and incident-response personnel of a large enterprise. VIAssist is a visualization technology that helps with the analysis of network traffic and security event data. It provides scalable representations of cyber data and aids in the discovery, analysis, and understanding of cyber attacks.
- The Security Innovation Network (SINET) Showcase and IT Security Entrepreneurs' Forum (ITSEF) Forum were held.

Project Performers

- ITT Exelis
- Security Innovation Network

Website

www.security-innovation.org

Program Manager

Dr. Douglas Maughan, *douglas.maughan@hq.dhs.gov*

LOOKING AHEAD TO FY 2012

S&T is an integral player in DHS's focus on safeguarding and securing cyberspace goals to ensure that the nation is prepared for the cyber threats and challenges of tomorrow.

The division's key research and development activities for FY 2012 will comprise five program areas:

- ***Research Infrastructure to Support Cybersecurity***
  - Launch an updated tool suite for the creation and analysis of cybersecurity experiments within the DETER testbed.
  - Release The Menlo Report, a guide for conducting ethical cybersecurity research.
- ***Trustworthy Cyber Infrastructure***
  - Work with the Mozilla Foundation, developer of the Firefox browser, to deploy a DNS-enabled Firefox for desktops and Android mobile devices.
  - Evaluate and release a public report on host-based cybersecurity technologies — specifically, technologies based on application whitelisting — that support continuity of operations in critical process-control system environments.
- ***Foundational Elements of Cyber Systems***
  - Initiate new research and development in support of the Comprehensive National Cybersecurity Initiative in areas such as Cyber Economics and Moving Target Defense.
  - Create a lessons-learned report on overcoming barriers to implementing open-source security technologies in government.
- ***Cybersecurity User Protection and Education***
  - Perform a proof-of-concept demonstration of the "verification of identity credential service" to improve identity-proofing procedures of potential financial account holders for the financial sector requirement.
  - Coordinate with state/local jurisdictions and the Federal Emergency Management Agency to demonstrate a standards-based attribute exchange capability for access control of emergency response officials at incident scene checkpoints.
  - Establish an assessment framework for national-level collegiate cyber competitions to develop a scoring coalition and identify top performers.
- ***Cybersecurity Technology Evaluation and Transition***
  - Identify federally sponsored research ready for transition to public and private partners, and formulate a transition plan for each.
  - Pilot a network visualization technology and open-source intrusion detection technology at S&T.

PERFORMER INDEX

PROJECT	PERFORMER	ROLE	PRIME CONTACT INFORMATION
Experimental Research Testbed	University of Southern California — Information Sciences Institute (USC-ISI)	Testbed Development and Operation	Terry Benzel tbenzel@isi.edu
Experimental Research Testbed	University of California — Berkeley	Testbed Development and Operation	
Experimental Research Testbed	Pacific Northwest National Laboratory (PNNL)	Process Control System Integration	
Experimental Research Testbed	University of Illinois at Urbana-Champaign (UIUC)	Process Control System Integration	
Research Data Repository	Packet Clearing House (PCH)	Data Host and Data Provider	Bill Woodcock woody@pch.net
Research Data Repository	University of Southern California (USC)	Data Host and Data Provider	John Heideman johnh@isi.edu
Research Data Repository	University of California — San Diego (UCSD)	Data Host and Data Provider	Kimberly (“kc”) Claffy kc@sdsc.edu
Research Data Repository	Research Triangle Institute (RTI)	Coordination Center Operations	Charlotte Scheper cscheper@rti.org
Research Data Repository	University of Michigan	Data Host and Data Provider	Michael Bailey mibailey@eecs.umich.edu
Research Data Repository	Global Cyber Risk, LLC	Legal Famework and Privacy Support	Jody Westby westby@mindspring.com
Research Data Repository	Merit Network, Inc.	Data Host and Data Provider	
Research Data Repository	Georgia Institute of Technology	Data Provider	
Research Data Repository	University of Wisconsin	Data Provider	
Secure Protocols — DNSSEC	Shinkuro, Inc.	Domain Name System Security (DNSSEC) Protocol Development	Steve Crocker Steve@shinkuro.com
Secure Protocols — DNSSEC	Sparta, Inc., a Parsons Company	Ubiquitous Deployment of Domain Name System Security	Russ Mundy Russ.Mundy@sparta.com
Secure Protocols — DNSSEC	National Institute of Standards and Technology	Border Gateway Protocol (BGP)	Douglas Montgomery DougM@nist.gov
Secure Protocols — SPRI	Sparta, Inc., a Parsons Company	Standards Development & System Prototyping	Sandra Murphy Sandra.Murphy@sparta.com
Secure Protocols — SPRI	Raytheon BBN Technologies	Standards Development & System Prototyping	
Internet Measurement and Attack Modeling	University of Southern California — Information Sciences Institute (USC-ISI)	Annotation and Mapping of Internet Topology at the Edges (Amite')	John Heidemann JohnH@isi.edu

PROJECT	PERFORMER	ROLE	PRIME CONTACT INFORMATION
Internet Measurement and Attack Modeling	University of California — San Diego (UCSD)	Leveraging the Science and Technology of Internet Mapping for Homeland Security	Kimberly Claffy KC@caida.org
Internet Measurement and Attack Modeling	Pacific Northwest National Laboratory (PNNL)	Project Management: Clique' and Traffic Circle	William Pike William.Pike@pnnl.gov
Internet Measurement and Attack Modeling	Colorado State University (CSU)	WIT: A Watchdog system for Internet Routing	Dan Massey Massey@cs.colostate.edu
Process Control Systems Security — LOGIIC	SRI International	Project Management	Ulf Lindqvist ulf.lindqvist@sri.com
Process Control Systems Security — TCIPG	University of Illinois at Urbana-Champaign (UIUC)	Project Director	Bill Sanders whs@illinois.edu
Homeland Open Security Technologies	Georgia Tech Research Institute (GTRI)	Project Lead	Joshua Davis Joshua.Davis@gtri.gatech.edu
Homeland Open Security Technologies	Open Source Software Institute	Solutions Inventory	
Homeland Open Security Technologies	Open Information Security Foundation	Software Development	
Software Quality Assurance	GrammaTech	Software Testing and Vulnerability Analysis	Paul Anderson Paul@grammatech.com
Software Quality Assurance	Applied Visions	Software Testing and Vulnerability Analysis	Ken Prole Ken.Prole@avi.com
Software Quality Assurance	Data Access Technologies	Software Testing and Vulnerability Analysis	Edwin Seidewitz ed-s@moledriven.com
Cyber Security Competitions	Center for Internet Security (CIS)	Highshcool Cyber Security Competitions	Karen Evans KarenEvans@prodigy.net
Cyber Security Competitions	University of Texas — San Antonio (UTSA)	Collegiate Cyber Security Competitions	Greg White Greg.White@utsa.edu
Cyber Security Forensics	ADF Solutions	First Responder Field Kit — Triage Responder	JJ Wallia, CEO/Co-founder info@adfsolutions.com
Cyber Security Forensics	Berla Corporation	GPS Forensic Logical Analysis Tool — Blackthorn3	Mike May, President/CEO mmay@berlacorp.com
Cyber Security Forensics	Carnegie Mellon University	Banking and Finance Sector Insider Threat Study	Dawn Cappelli dmc@cert.org
Cyber Security Forensics	ITT Exelis	Law Enforcement Information Portal — CyberFETCH	Salvatore C. Paladino sal.paladino@exelisinc.com
Cyber Security Forensics	National Institute of Standards and Technology	National Software Reference Library/Cyber Forensics Tool Testing	Barbara Guttman barbara.guttman@nist.gov cftt@nist.gov nsrl@nist.gov
Cyber Security Forensics	Purdue University	Disposable Mobile Phone Analysis Study	Marc Rogers rogersmk@purdue.edu

PROJECT	PERFORMER	ROLE	PRIME CONTACT INFORMATION
Cyber Security Forensics	University of Tulsa	Physical Extraction and Reconstruction of Evidence from Mobile Phones	Sujeet Shenoi *sujeet@utulsa.edu*
Cyber Security Forensics	University of Wisconsin	Vulnerability Assessment of Open Source Wireshark	Prof. Barton P. Miller *bart@cs.wisc.edu*
Identity Management — Identity and Access Management	Johns Hopkins University - Applied Physics Laboratory	Host the Identitiy Management Testbed; Backend Attribute Exchange	Shameeka Hunt *shameeka.hunt@jhuapl.edu* Tom Smith *tom.smith@jhuapl.edu*
Identity Management — Identity and Access Management	Queralt	Small Business Innovation Research effort "Interoperable Attribute-based Physical Access Control"	Michael Queralt *michaelq@queraltinc.com*
Identity Management — Data Privacy Technologies	MITRE SEDI	Support for the Privacy Working Group	Stuart Shapiro *sshapiro@mitre.org*
Identity Management — Data Privacy Technologies	Massachusetts Institute of Technology	Prototyping Fusion Center Information Sharing; Implementing Policy Reasoning Over Cross-Jurisdictional Data Transactions Occurring in a Decentralized Environment	Hal Abelson *hal@mit.edu*
Distributed Environment for Critical Infrastructure Decision-Making Exercises	Norwich University Applied Research Institutes	Program Lead	Andy Cutts *andy@cybstrat.com*
Cyber Security Assessment and Evaluation	ITT Exelis	Technology Assessment and Evaluation	Sal Paladino *sal.paladino@exelisinc.com*
Cyber Security Assessment and Evaluation	Security Innovation Network	Liaison with private sector; relationship building	