

# **What Works in Implementing the US National Strategy to Secure Cyberspace Case Studies of Success in the War on Cybercrime and Cyber Espionage A SANS Consensus<sup>1</sup> Document**

Version 1.0 December 10, 2007

*Public Comment Period: This document is posted at [www.sans.org/fedsuccesses](http://www.sans.org/fedsuccesses) for a 29-day comment period. In that time the authors hope additional successes will be documented and any factual errors in the current set will be corrected. Send additions/comments/corrections to [apaller@sans.org](mailto:apaller@sans.org) no later than February 8, 2008. The final report will be released on February 14, the anniversary of the **National Strategy**.*

As the **US National Strategy to Secure Cyberspace** approaches its fifth anniversary, prudence dictates that the nation measure what has been accomplished under that strategy to determine which efforts should be continued and enhanced, and which need to be altered or discarded.

The successes of the projects described in this paper for securing the nation's cyber infrastructure are worthy of our praise. In fact, they are critical to national security and should be adopted more broadly. However, as we acknowledge these successes, it's also essential to acknowledge that the level and sophistication of cyber threats are increasing. Organized crime groups in Eastern Europe and Asia are spending hundreds of millions of dollars each year to buy exploits and recruit and employ the best hackers in the world; they are leading a \$10 billion financial crime spree. Terrorists are using money stolen from US banks, through cyber fraud, to pay for the bombs that kill innocent people around the world. Certain rogue nation states have concluded that their very survival depends on their ability to penetrate and corrupt US government computers, and they have been enormously successful in infiltrating computers at the Department of Defense (DoD), military contractors, Department of Energy (DoE) labs, the State and Commerce Departments and more. Even the Department of Homeland Security's (DHS's) own computers are not immune and have suffered breaches in their environment.

Clearly much more needs to be done to slow the tidal wave of cybercrime. We hope that the successes illuminated here will serve as prototypes to demonstrate that government leadership by example is both possible and effective.

## **Measures of Success**

Projects were selected for inclusion only after determining that there is evidence of substantial and measurable improvement in the US capacity to meet one or more of the three strategic objectives that shape the **National Strategy to Secure Cyberspace**:

1. Prevent cyber attacks against America's critical infrastructures;
2. Reduce national vulnerability to cyber attacks; and
3. Minimize damage and recovery time from cyber attacks that do occur.

The evidence of each project's impact needed to be direct, substantial, and measurable since any other criteria would result in the inclusion of an enormous number of ineffective initiatives, most of which have also been very expensive. For example, the Department of Homeland Security's Cyber Storm I national exercise in 2006 might be considered by some to have been a success. It was not included in this list because no substantial, measurable change in behavior or effect can be attributed to it. We may have learned some lessons from the exercise, but there is no substantial evidence to indicate an intent to act on those lessons. On the other hand, the deployment of DoD's Common Access Card (CAC) resulted in a large decrease in the opportunity for unauthorized access to government computers. Similarly, the National SCADA (Supervisory Control and Data Acquisition) Test Bed and the Control Systems Security Program have already substantially and measurably improved the security of systems that control much of the nation's most critical infrastructures.

In the policy arena, substantial advances have been made, ranging from the ratification of the Council of Europe Cybercrime Convention, to the appointment in DHS of an Assistant Secretary with primary responsibility in cyber security, to the addition of a cyber security sidebar to the Homeland Security Strategy. These advances help shape the landscape of cyber security, but it is nearly impossible to show that they have resulted in significant improvement in any of the three strategic objectives of the *National Strategy*.

For each successful initiative, we describe 1) the challenge it met; 2) the organizations that acted to make it happen; 3) what they did and how they did it; 4) how we know it worked and; 5) an estimate of procurement and operating costs.

### **1. THE CHALLENGE: Decrease the security vulnerabilities of millions of federal computers while reducing procurement and operating costs.**

**Federal government agencies spend tens of millions of dollars trying to configure their computers safely and then hundreds of millions more testing and deploying system and security patches as they become available. Even with spending in the multiple millions of dollars, most federal computers do not have consistently secure configurations and most federal agencies take weeks or months to patch their systems. This allows fast-moving cyber attackers the ability to exploit the vulnerabilities before the patches are installed. An analysis by NSA, published in 2002, found that as many as 90% of all vulnerabilities are eliminated through up-to-date patching and secure configuration.**

*Who:* The U.S. Air Force (USAF), National Security Agency (NSA), Defense Information Systems Agency (DISA), National Institute of Standards and Technologies (NIST), DHS, and the Office of Management and Budget (OMB), plus the Center for Internet Security (CIS), Microsoft, and Dell.

*What:* A standard desktop operating system configuration with integrated security, deployed on over 450,000 computers.

The most important success in federal government cyber security to date is the Federal Desktop Core Configuration (FDCC) and its predecessor proof-of-concept project in the U.S. Air Force.

The Air Force, with the help of NSA, NIST and DISA, created a standard configuration of two popular Windows operating systems and then used its procurement power to ensure all relevant computer suppliers delivered computers with the secure configuration installed at the time of delivery. The result was radically reduced costs for implementing security because the standard security configurations were built-in by the vendors. Additional savings were experienced in patch testing and user support since the resources required for these operational activities were significantly reduced. The Air Force proved that procurement, using well-vetted standard configurations, can improve the overall security posture while lowering procurement and operating costs. The Air Force also tested the hypothesis that implementing secure configurations would cause software applications to break. What they learned was that only a few legacy applications were impacted and then only if those applications required users to run the applications with elevated privileges (a particularly dangerous practice because it puts the system at increased risk of being compromised by remote cyber-attackers).

*How effective is this initiative in the U.S. Air Force?* Lieutenant General Michael Peterson, Chief of Warfighting Integration and USAF CIO, told *Military Information Technology* magazine, “[the initiative is] reducing our network patch time from 57 days to less than 72 hours while simultaneously cutting the workload for system administrators in half. Ultimately this reduces the cost of software licensing by over \$100 million across the FYDP”. And of course, faster system patching makes it more difficult for hackers to breach critical systems, resulting in lower costs AND improved cyber security.

The Office of Management and Budget (OMB) actively followed the Air Force experiment from the beginning. When the Air Force project proved successful, OMB leadership issued instructions for all federal agencies to standardize on the secure Air Force configuration as adjusted by NIST. OMB also proactively resolved potential application incompatibility problems by issuing a mandate that no software can be purchased that: 1) doesn’t run on the secure operating system configuration or: 2) requires elevated privileges.

*The result:* Federal agencies gain improved security configurations, faster system patching and lowered procurement and operating costs. Active leadership in the federal government made it viable for Microsoft to create configurations of Windows that are much more secure than standard Microsoft operating system configurations, ultimately, as Microsoft makes the same secure configurations generally available, enabling buyers throughout the world to gain the same benefits of improved security and lower costs.

This project also illustrates how the public-private partnership can work. First, the National Security Agency and the Center for Internet Security (a public-private partnership composed of more than 100 private companies and US and international government members) developed a consensus draft secure configuration for Windows and other operating systems and applications. The Windows configurations were honed by the USAF, Microsoft, NIST, DISA and NSA to become the Federal Desktop Core Configuration (FDCC). Once the configuration was tested and validated, Microsoft, Dell and other PC vendors contracted with the government to deliver the securely configured versions of Windows operating systems. Prior to the creation of the FDCC, these vendors actually wanted to deliver more secure systems but it was too difficult and expensive when every enterprise had its own definition of the ‘right’ configuration. This project

made it possible for system vendors to meet their business objectives AND deliver systems that actually improved security.

Lesson Learned: In procurement, scale means leverage. The combined software budget of the Air Force was substantial. Microsoft and Dell were able to deliver the common configuration easily because the cost of development and deployment could be spread over hundreds of thousands of copies of the software. The combined budgets provided leverage with the appropriate incentives for them to further reduce costs for baking security into the systems they deliver to government and industry.

*How much did it cost?* Developing the benchmark configurations cost approximately \$2.4 million, and initial testing of the new configurations at the USAF cost another \$500,000 but the implementation of those configurations actually saved money. The Air Force saved \$100 million in software procurement costs by consolidating its procurement across 38 legacy contracts. Additional tens of millions of dollars are being saved in reduced system administration and help-desk costs every year.

**2. THE CHALLENGE: Identifying cyber attacks on federal agencies and illuminating federal systems that have been corrupted by cyber attackers. This is especially important in an age of botnets where increasing numbers of federal systems are infected through spear phishing and then used to attack other organizations or to steal sensitive information.**

*Who:* The National Cyber Security Division of the US Department of Homeland Security, National Security Agency, Office of Management and Budget , CERT/CC at Carnegie Mellon University, and several cabinet-level agencies.

*What:* The Einstein program: enables full-time monitoring and analysis of network traffic received and sent by federal agencies resulting in identification of patterns that may be signs of persistent presence of unauthorized software and users on federal networks. Its expansion into the Trusted Internet Connection (TIC) program extends these benefits to all federal agencies.

Fourteen federal agencies have already deployed Einstein sensors at their network gateways to capture information about network traffic and feed it to analysis programs run by CERT/CC at Carnegie Mellon University in Pittsburgh on behalf of the US Department of Homeland Security. In a dramatic demonstration of the promise of the deployment, network traffic transmitted by the Department of Agriculture and received by the Einstein sensors at the Department of Transportation contained malicious packets that indicated Agriculture systems had been penetrated and infected. The Einstein analysts quickly contacted Agriculture and helped that agency find and eliminate the infection. This is just one of numerous similar examples of Einstein's ability to find infected systems inside agencies.

Under the new Trusted Internet Connection program, federal agencies will reduce the number of Internet connections and ensure all traffic is monitored through the Einstein analytical systems.

*How much did it cost?* Einstein cost \$33 million over the past three years and an additional \$14 million per year. TIC will cost hundreds of millions.

**3. THE CHALLENGE: Improving the security of industrial control systems at nuclear power plants, utilities and other critical infrastructure elements in both the government and private sectors.**

**Supervisory Control and Data Acquisition (SCADA) and other control systems often last 20 to 30 years, and most industrial control systems were designed and installed before cyber security threats were known or widely understood. Utilities have now come under direct attack and some facilities have even been subject to extortion demands by hackers who have broken through the defenses. Thousands of public and private sector organizations need to move quickly toward improving the security of these critical systems.**

*Who:* The Department of Energy; Department of Homeland Security; the State of New York, the Idaho National Laboratory (INL), Sandia National Laboratory (SNL), and Pacific Northwest National Laboratory (PNNL), plus a consortium of control system vendors.

*What:* The National SCADA Test Bed and the Control Systems Security Program and the SCADA Security Procurement Specifications.

Government Accountability Office (GAO) reports in March 2004 (<http://www.gao.gov/new.items/d04354.pdf>) and September 2007 (<http://www.gao.gov/new.items/d071036.pdf>) document “increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks” against the control systems that manage power plants, electric distribution systems, oil and gas pipelines, water systems, transportation systems, and dams. Reliance on technologies from the 1960s and 1970s, combined with increasing use of newer Windows operating systems and insecure direct and wireless connections of control systems to external networks, have led to substantial vulnerabilities within the nation’s critical industries.

The most important success in building a public-private partnership to improve cyber security has been the national effort to secure control systems. The National SCADA Test Bed team assembled a representative group of control systems from most major suppliers and performed in-depth vulnerability tests on those systems. Their testing was sophisticated and comprehensive and the vulnerabilities they found were both important and common across vendor systems. When the Test Bed team finds significant vulnerabilities, INL engineers demonstrate the problem to the system manufacturer. These manufacturers then correct the problem when possible and INL engineers verify that the vulnerability has been eliminated. The vendors are then able to deliver the corrected system to each new customer and sometimes fix the vulnerability in existing systems. Federal funds were significantly augmented with funding from manufacturers and asset owners who wanted to support the Test Bed and ensure testing went beyond those funded by federal agencies.

Vulnerabilities discovered by the testers need to be corrected in all control systems. DHS and DoE funded INL to develop and distribute procurement specifications that utilities in the US and around the world are already using to ensure their control system vendors are delivering baked-in security. With the assistance of the Multi-State Information Sharing and Analysis Center, led by New York State, and the United Kingdom's Centre for the Protection of the Critical National Infrastructure (CPNI), these specifications are being adopted in the US and are being considered for formal adoption by a ten-country consortium.

*The result:* Many vulnerabilities in control systems have been found and corrected, and, using the new procurement specifications, buyers of SCADA and control systems can tell vendors exactly what is needed and ensure important vulnerabilities are eliminated.

*How much did it cost?* The National SCADA Test Bed and Control Systems Security Program cost approximately \$17 million annually in federal funds over the past four years (funds that have been cut back sharply in the current year) and more than \$4 million in private funding (contributions of equipment for testing, for example) by control system vendors and utilities in support of testing and where industry needed additional testing not funded by the federal programs.

#### **4. THE CHALLENGE: Raising international barriers and increasing criminal penalties for cybercrime by identifying and capturing more cyber criminals and incarcerating them for longer periods.**

**Cyber criminals live and work in many countries. When one of those countries has weak laws against hacking or when that country's law enforcement organizations have neither the skills nor the will to pursue hackers attacking foreign systems, the criminals know they can operate with impunity. Even where cybercrime is illegal, sentences for convicted cyber hackers were very lenient -- often simply probation.**

*Who:* The Justice Department's Computer Crime and Intellectual Property Section (CCIPS), the FBI's Cyber Security Program, and the cyber security programs of the US Secret Service and the US Postal Inspection Service.

*What:* 1) Bilateral and multi-lateral agreements between law enforcement groups in the US and other countries allowing immediate capture of cyber criminals through real-time cooperation; 2) Better education of prosecutors, investigators and judges about how to investigate and prosecute cybercrime cases and the damage to businesses and other organizations caused by cybercrime; 3) Improved law enforcement techniques and tools to identify and capture more criminals and; 4) the National Cyber-Forensics and Training Alliance (NCFTA).

The US Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) has attempted to standardize cybercrime law internationally through the development and support of the Council of Europe's Convention on Cybercrime. CCIPS used active diplomacy to provide technical assistance to countries around the world to help them synchronize their cybercrime laws, and, with the help of federal investigative agencies, helped them build much stronger cyber

law enforcement capabilities. In addition, by developing and maintaining the G8 Hi-Tech Crime Subgroup's 24/7 Points of Contact Network involving 50 nations, CCIPS facilitated a means of expediting requests for, and responses to, international needs for assistance in urgent cybercrime matters. CCIPS also created the Computer Hacking and Intellectual Property (CHIP) Network of approximately 230 Assistant United States Attorneys (AUSAs) around the country. The CHIP Network coordinates investigations and provides training, knowledge, and assistance on the prosecutions of computer and intellectual property crimes to AUSAs in United States Attorneys' offices throughout the country.

At the same time, the FBI built cyber squads in dozens of field offices and established legal attaché offices ("legats") in 60 countries around the world. Those squads and international law enforcement partners supported by the legats have had impressive success in finding and capturing cyber criminals. In parallel with these efforts, the FBI has put a dozen full-time cyber investigators into a facility that also houses representatives of universities and more than a dozen leading US corporations. The public-private initiative, called The National Cyber-Forensics and Training Alliance (NCFTA), has accounted for the identification of more than 1,900 phishing drop sites (where the victims' data are stored), resulting in the prevention of tens of millions of dollars in losses. NCFTAs' work also led to the recent arrest of several dozen people involved in international credit card fraud enabled by cyber-theft of private information.

The US Secret Service and the US Postal Inspection Service also played huge roles in many major, successful cyber investigations and are pillars of the national initiative to make cyber criminals pay for their crimes.

*The result:* Law enforcement officials have had many more successful investigations and prosecutions of cyber criminals, and judges have been meting out much longer sentences – six years or more in some recent trials. That's up from less than a year just five years ago. All of this has helped send a good deterrent message that is essential to securing cyberspace.

*How much did it cost?* Because almost every major crime today has a cyber dimension and nearly all cybercrime has an international dimension, it's impossible to calculate the cost of this important initiative. The NCFTA costs \$1.5 million per year (in addition to the salaries of the federal investigators).

## **5. THE CHALLENGE: Making remote exploits of federal computers more difficult by ensuring that only authorized users gain access. User names and passwords are insufficient to ensure that only authorized people are using computers.**

*Who:* Department of Defense (DoD), GSA, OMB and most federal civilian agencies.

*What:* Implementing two-factor authentication for all personnel requiring access to government computer systems.

The US Department of Defense distributed Common Access Cards (CAC) enabling the DoD to ask every would-be user of its networks and computer systems to have a card in his or her

possession and to know a personal identification number or password. Requiring two different forms of identification – one the user has in his or her physical possession and one the user knows, is called two-factor authentication. Two-factor authentication is a proven method for decreasing intrusions and other types of security breaches by ensuring that stolen user names and passwords are insufficient to gain access to networks.

DoD's success with its Common Access Card led the US Office of Management and Budget to issue Homeland Security Presidential Directive 12 (HSPD-12), requiring all federal agencies to implement two-factor authentication. As agencies fully implement HSPD-12, they will gain the same benefits that DoD has obtained.

*The result:* On January 25, 2007, Lt. General Charles Croom, USAF, told an audience in Colorado Springs, "Although there are six million probes of Defense Department networks a day, successful intrusions have declined 46 percent in the past year because of a requirement that all DoD personnel log on to unclassified networks using Common Access Cards."

Large-scale procurement of Common Access Cards by DoD and emerging procurements by other federal agencies under HSPD 12 has already reduced the cost of deployment from over \$100 to less than \$50 per card.

*How much did it cost?* The DoD Common Access Card program cost more than \$6 million just for the R&D process and then tens of millions more for deployment. HSPD-12 implementation to date has cost in excess of \$100 million.

## **6. THE CHALLENGE: Safeguarding sensitive data stored on mobile (laptop) computers from loss or theft.**

**Tens of thousands of government computers have been lost or stolen and the data on many of those systems were unprotected and unencrypted. The embarrassment to federal agencies has been acute and senior officials have been consumed by responding to Congressional inquiries and press questions.**

*Who:* DoD, GSA, Office of Management and Budget, and the Multi-State Information Sharing and Analysis Center.

*What:* SmartBuy provided federal government agencies with a low-cost acquisition vehicle for laptop encryption software and extends the benefits of that procurement to state and local governments.

Encrypting the data on mobile devices (laptop computers, PDAs and cell phones) makes sense but encryption software and hardware are expensive. Consequently, most organizations have been unable to commit to widespread implementation. The economics of software offers an easy solution but it requires a catalyst to make it happen. The cost of making each additional copy of a software package is very low, so if a software vendor is assured of selling vast numbers of additional copies, that vendor can lower the price and still earn potentially greater profits. One

buyer has to be first to prove that the number of copies to be sold is very large. In this project, the Federal SmartBuy program proved to software vendors that they can lower prices substantially when volumes are large enough.

*The result:* Under the old GSA contract, federal agencies could buy, for example, SafeBoot, a popular full-disk laptop encryption product, for \$99 per copy in quantities under 100. When an agency buys 5,000 to 10,000 copies, the price is \$81.99 per copy. Most agencies that buy more copies have been able to push the prices down to between \$55 and \$60 per copy. But in September 2007, under the new large-volume SmartBuy initiative, the Department of Agriculture bought 180,000 copies of encryption software for \$1.8 million or \$10 per copy. In other words, consolidated federal buying power guaranteed sufficient quantities that enabled the software vendor to provide discounts of nearly 90%, and still earn a healthy profit. This example of federal procurement leadership is especially important because the US government contracting initiative enabled state and local governments to also buy software under the new contract. This allowed fiscally strapped small government organizations to buy five to ten times as many copies of encryption software for the same price they would have had to pay without federal procurement leadership.

*How much did it cost?* The effort to create the SmartBuy contract cost about \$300,000 but the resulting savings are huge. Just at the Department of Agriculture, the direct savings exceeded \$7 million.

## **The Most Promising Federal Cyber Security Program on the Horizon**

**THE CHALLENGE: Improving the ability of agencies to keep their systems patched in the face of a flood of new vulnerabilities that exceeds human capacity to find and fix before systems are exploited.**

*Who:* The National Security Agency (NSA) and the National Institutes for Standards and Technology (NIST), Microsoft and other commercial system and security software vendors.

*What:*, The Security Content Automation Program (S-CAP) will make it possible to automate the entire chain of events from vendors reporting vulnerabilities and how to find them, to vulnerability testers finding the flaws, to system managers and configuration software programs recording the full state of each system, ultimately to patching tools actually correcting the problems, all in real time, without human intervention.

This is one of the most promising projects in cyber security because it engages all the players, from application and system software developers to system management tool suppliers to security tool suppliers, to upgrade their tools so they can work together to protect federal and other critical systems. It promises to radically lower the cost of maintaining security “hygiene” and promises a future in which security professionals focus on other problems.

*How much did it cost?* Approximately \$12 million to date but the amount will grow substantially when commercial organizations re-engineer their processes and software to use the

automated protocols. On the other hand, once S-CAP is fully operational, agencies and industry can expect substantial cost reductions because they will be able to eliminate much of the manual effort currently associated with finding and fixing vulnerabilities in the software they have deployed.

*Why is it promising and not yet a full success?* S-CAP has not yet been implemented in enough commercial tools to enable full automation.

==end==

---

<sup>i</sup> The authors of this document are Alan Paller of the SANS Institute, Paul Kurtz of Goodharbor, Jim Lewis of the Center for Strategic and International Studies, John Gilligan of SRA, and Frank Reeder. Others who provided valuable input include Will Pelgrin of New York State, Christopher Painter of the US Department of Justice, MarjoriyBlumenthal of Georgetown University, Ed Skoudis of Intelguardians, Mark Weatherford of the State of Colorado, Clint Kreitner of the Center for Internet Security, Marcus Sachs of Verizon, Eugene Schultz of High Tower, and Mason Brown, Johannes Ullrich, Stephen Northcutt and Eric Cole of the SANS Institute.