HOMELAND SECURITY ADVISORY COUNCIL

CYBERSKILLS TASK FORCE REPORT
FALL 2012

PREFACE

The cyber threat facing the nation has escalated sharply in recent years and come into clear focus.

In April 2009, the *Wall Street Journal* ran a front page article entitled "Electricity Grid in U.S. Penetrated by Spies,"[1] and CNN showed proof that a cyber attack can cause a power generator to break apart.[2]

At the same time, the technological wealth of Western nations continues to be systematically stolen through cyber attacks. In a private letter to the managing directors of the 300 largest companies in the United Kingdom, MI5 Director-General Jonathan Evans told the business leaders that their networks and systems, as well as those of their attorneys and advisors, were being penetrated with the same advanced attack techniques used to steal military secrets from defense agencies.[3]

Federal civilian agencies have not been immune. Computers have been penetrated in the Bureau of Industry and Security, the U.S. Commerce Department agency responsible for holding data on "technologies too sensitive to export."[4]

DHS's own systems have been under attack. In 2007, DHS CIO Scott Charbo testified that more than 840 cyber-related incidents—many involving malicious software designed to set up back doors to steal information and make changes to agency systems—had occurred during the two previous fiscal years and were continuing.[5] A massive hacking attack in 2008 that impacted over 500,000 pages on websites worldwide infected a DHS website. Every visitor to the DHS site was sent malicious software designed to take over their computer and turn it into a zombie to distribute spam or attack other computers.[6] While DHS detected and cleaned up the site the same day, the message was clear that the Department needed to deploy practices that were more aware, secure, nimble, and responsive to the growing volume and sophistication of cyber attacks.

Upon taking office in 2009, DHS Secretary Janet Napolitano recognized the urgency of the situation. In October of that year she announced a new excepted service hiring authority to enable DHS "to recruit the best cyber analysts, developers and engineers in the world to serve their country by leading the nation's defenses against cyber threats."[7] Gaining Office of Personnel Management approval for the hiring authority promised a rapid build-up of knowledgeable cybersecurity staff at DHS.

Within months of Secretary Napolitano's announcement, however, a new and sophisticated wave of attacks against U.S. industry was revealed. Google announced that it, along with more than 70 high-tech companies, had lost important intellectual property.[8] Exxon-Mobil, Marathon, and Conoco-Phillips also revealed their systems had been penetrated by sophisticated nation-state actors.[9]

These sophisticated attacks are the new norm, even penetrating the most protected, classified networks maintained by the U.S. military in a combat zone.[10] Intrusion prevention suppliers reveal privately that their systems are unable to keep up with the sophistication of attacks, and anti-virus companies report that attackers are reverse-engineering the vendors' anti-virus software and building new viruses so sophisticated that the tools cannot stop them.[11] Nor is the problem going away anytime soon—multiple sources have reported a sharp rise in attacks over the past six months; specific reports indicate a 200% increase in attacks and a spread to many organizations that have not previously been targets of nation-state attacks.[12]

In the face of such burgeoning threats, DHS has determined to move immediately to the next level of capability, one built upon the very advanced technical skills necessary to not only respond to but get ahead of this new attack tempo.

Finding the people with the needed skills, however, poses a dilemma. The numbers of professionals with these mission-critical skills are so limited that government contractors and federal agencies compete with one another and the private sector to hire them. Not surprisingly, a recent article in Bloomberg News reports that "the competition is fiercest for workers with hands-on experience defending systems against hackers and malicious viruses that can steal sensitive government data."[13] For DHS to acquire sufficient talent in such a competitive environment, it needs to radically expand the national pipeline of professionals with sophisticated technical cybersecurity skills.

On June 6, 2012, Secretary Napolitano announced the formation of a Task Force on CyberSkills with a two-part mandate: first, to identify the best ways DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges; and second, to outline how DHS can improve its capability to recruit and retain that sophisticated cybersecurity talent.

The Task Force on CyberSkills report is presented here. Secretary Napolitano gave the Task Force broad access inside DHS to gather data to better understand what has already been done and what needs to be done. This report identifies the models and resources throughout government and industry that will enable action to meet the cyberskills mandate. If implemented, its recommendations will not only expand the national pipeline of men and women with advanced cybersecurity skills, but will also enable DHS to become a preferred employer for the talent produced by that pipeline, positioning the Department to help make the United States safer, more secure, and more resilient.

Recommendations of the DHS Task Force on CyberSkills

In this report, the Department of Homeland Security's Task Force on CyberSkills proposes far-reaching improvements to enable DHS to recruit and retain the cybersecurity talent it needs. At the same time, the report proposes ways to boost the nation's overall ability to develop professionals with the advanced cybersecurity skills needed to protect the information, systems, and networks that enable effective and secure operation of government and commercial elements of critical national infrastructure.

In her *Blueprint for a Secure Cyber Future* presented in November 2011, Secretary Napolitano wrote that one day in the future "federal agencies and private sector entities will have the technical cybersecurity workforce needed to meet their mission responsibilities."[14]

For DHS and the nation's cybersecurity, the future is now.

Five Key Objectives That Will Be Met by Implementing the Task Force Recommendations

The eleven recommendations of the DHS Task Force on CyberSkills are grouped under five objectives:

Objective I: Ensure that the people given responsibility for mission-critical cybersecurity roles and tasks at DHS have demonstrated that they have high proficiency in those areas.

- Recommendation 1: Adopt and maintain an authoritative list of mission-critical cybersecurity tasks (Page 6).
- Recommendation 2: Develop training scenarios that enable evaluation of mission-critical cybersecurity talent for each of the mission-critical tasks (Page 9).
- Recommendation 3: Adopt a sustainable model for assessing the competency and progress of the existing and future DHS mission-critical cybersecurity workforce (Page 10).

Objective II: Help DHS employees develop and maintain advanced technical cybersecurity skills and render their working environment so supportive that qualified candidates will prefer to work at DHS.

- Recommendation 4: Establish a Department-level infrastructure with direct responsibility for the development and oversight of the cybersecurity workforce (Page 12).
- Recommendation 5: Make the hiring process smooth and supportive and make mission-critical cybersecurity jobs for the federal civilian workforce enticing in every dimension: in mission and service, skills, growth potential, and "total value proposition" (Page 14).

Objective III: Radically expand the pipeline of highly qualified candidates for technical mission-critical jobs through innovative partnerships with community colleges, universities, organizers of cyber competitions, and other federal agencies.

- Recommendation 6: Establish a two-year, community-college-based program that identifies and trains large numbers of talented men and women to prepare them for mission-critical jobs in cybersecurity (Page 17).
- Recommendation 7: Raise the eligibility criteria for designation as CAE and SFS schools to ensure that graduates are prepared to perform technical mission-critical cybersecurity jobs (Page 19).
- Recommendation 8: Launch a major, sustained initiative to enhance the opportunities for U.S. veterans to be trained for and hired in mission-critical cybersecurity jobs (Page 21).

Objective IV: Focus the large majority of DHS's near term efforts in cybersecurity hiring, training, and human capital development on ensuring that the Department builds a team of approximately 600 federal employees with mission-critical cybersecurity skills.

- Recommendation 9: Until 600 employees are on board with mission-critical skills, apply the large majority of direct hire authority related to information technology in the Department to bringing on people with technical mission-critical cybersecurity skills (Page 22).
- Recommendation 10: Specify the mission-critical skills and level of proficiency needed in all cybersecurity-related contracting (Page 23).

Objective V: Establish a "CyberReserve" program to ensure a cadre of technically proficient cybersecurity professionals are ready to be called upon if and when the nation needs them.

- Recommendation 11: Establish a pilot DHS CyberReserve program that ensures DHS cyber alumni and other talented cybersecurity experts outside of government are known and available to DHS in times of need and determine how this program may be implemented long-term (Page 24).

Objective 1: Ensure that the people given responsibility for mission-critical cybersecurity roles and tasks at the Department of Homeland Security have demonstrated that they have high proficiency in those areas.

The Challenge: Better define the mission-critical work force needed at DHS and reliably assess the skills of job candidates and current staff with cybersecurity responsibilities.

In her tasking letter posing this challenge, Secretary Janet Napolitano said that DHS needs a "workforce with specialized knowledge and skill" to carry out its mission.[15] The Task Force's first job was thus to identify those specialized skills without which DHS cannot meet its cybersecurity responsibilities (called "mission-critical tasks" and "mission-critical skills"). Explicit definitions of the required skills are needed to enable DHS to differentiate between people who actually have those skills and people who may have knowledge in the area but no hands-on skills. Explicit definitions are also essential to meet the Task Force's charge to identify the most promising and effective competitions, university programs, internships, private sector programs, and relevant federal government programs that may be valuable as partners or sources of talent for the Department.

The Task Force found that DHS needs to expand the number of its federal employees with hands-on, advanced cybersecurity skills for the mission-critical tasks listed in Table 1. This expansion is necessary for two reasons: first, critical skills have not been properly specified to reflect the newly emerging threat, making it difficult for the Department to hire people with the necessary hands-on skills and expertise to perform at the level needed to defend against increasingly sophisticated threats. Second, in order to respond quickly to increasing cybersecurity needs, DHS has used contractors for many of the "cool" hands-on jobs, from penetration testing to reverse engineering and security engineering—leaving fewer of these sought-after positions open to federal employees.

This is an urgent problem. In order for the Department to appropriately meet the needs of industry and government, perform its mission-critical tasks, and provide sufficiently technical direction to properly drive contractor support efforts, we believe the Department needs at least 600 federal workers who have the technical cybersecurity skills to handle mission-critical tasks.

We set this initial target of 600 technical cybersecurity specialists based on comparisons with other large organizations, but anticipate that the number will be adjusted when the Department completes the enterprise-wide review that is currently under way of the numbers and competencies of its existing technical cybersecurity workforce and of its workforce requirements.[16]

How can DHS measure the proficiency of the candidates or staff it evaluates to fill mission-critical jobs? If these jobs are essential to protect the nation, then the answer must be through stringent and ongoing evaluation of proficiency, similar to that used for such professions as pilots, physicians, and nuclear plant operators. All of those professionals must pass proficiency exams not once but regularly—as often as every six months for some pilots—in

order to keep their jobs.[17] The standards are strict because people's lives depend on these professionals doing their jobs effectively. Certainly the risks of malicious actors penetrating the computer systems of America's power systems, or hostile nations stealing U.S. military and economic secrets, rise to a similar level of urgency. It is thus incumbent on DHS to set a high bar for technical proficiency for any DHS employee seeking a position of responsibility that involves providing technical guidance and cybersecurity incident response support to the nation's critical infrastructure and civilian government agencies. That means using techniques as rigorous as those used for the professions mentioned above, including scenario-based testing to measure proficiency.

This core idea of defining and using very specific mission-critical skills and scenario-based testing/training meets a critical need felt across government and industry. DHS success here would ripple across the entire industry and reinforce DHS leadership in cybersecurity.

Adoption of the following three recommendations will enable the Department of Homeland Security to rapidly meet the challenge to better define its mission-critical work force as well as reliably and continuously assess the skills of job candidates and current staff with cybersecurity responsibilities.

Recommendation 1: Adopt and maintain an authoritative list of mission-critical cybersecurity tasks.

Many DHS jobs and tasks are essential, but the Department has shortages of federal employees with the skills needed to perform the mission-critical tasks listed in Table 1. The Task Force members believe that DHS cannot be the nation's nerve center for ensuring a secure and resilient infrastructure without closing those specific mission-critical skill gaps.

To implement this recommendation, the Department should establish an authoritative list of mission-critical jobs and tasks and keep it current in the face of changing threats and technologies.

Table 1 presents the Task Force's recommended list of mission-critical jobs and tasks and the consequences if they are not executed effectively.[18] Recommendation 4 establishes the internal DHS Cyberworkforce Board empowered to keep the list of mission-critical cybersecurity tasks current with the changing threat landscape.

The first two jobs in Table 1, "network and system penetration testing" and (2) "application penetration testing," provide an effective on-ramp for initiating a major skills development program at DHS. The tasks performed by people in both of these jobs have three characteristics that make them promising starting points for building advanced mission-critical skills: (1) These are baseline tasks that produce better technical skills in the other task areas—that is, knowing how to penetrate an architecture allows for better security monitoring, event analysis, security engineering, and architecture, and knowing how to find and exploit application vulnerabilities allows for better code reviews, forensics analysis, threat analysis, and incident response; (2) Results of penetration tests are immediately

relevant and motivating for the agencies and companies that DHS helps to support, enhancing trust in the Department's reputation for cybersecurity excellence; and (3) These are the most stimulating and "coolest" jobs that candidates for employment consistently seek. Having significant numbers of these jobs reserved for federal employees will help DHS compete effectively with other employers for top talent and serve as a pipeline for the other skills the Department needs to meet its cybersecurity mission.

Job	Tasks	Consequences of Failure to Perform
System and network penetration tester	Follow a systematic process to assess the ability of systems and networks to withstand sophisticated adversaries who have knowledge of the architecture and systems that are deployed. This is not social engineering or running a vulnerability testing tool or a packaged exploit tool, but rather a sophisticated technical testing of the configuration and pathways and interactions between systems that mimics the techniques employed by advanced adversaries.	System configuration and composition weaknesses may be exploited by advanced adversaries and insiders for data exfiltration and to take over command-and-control of internal systems and processes. Failure to have extensive programs in this area also eliminates a valuable skill development program. Knowing how to penetrate an architecture enables better security monitoring, event analysis, and security engineering, and architecture.
Application penetration tester	Test applications before they are deployed and when they are modified. Identify the avenues that are most riddled with flaws and holes and that give malicious actors access to the most important content or systems. This is not only a tool-deployment task; it also requires deep understanding of the application being tested.	Applications will be deployed, particularly on the web, that can be exploited and made to infect visitors' computers, deeply embarrassing the agency, or that can be used as access pathways for data exfiltration. Failure to have extensive programs in this area also eliminates a valuable skill development program. Knowing how to find and exploit an application vulnerability allows for better code reviews, forensics analysis, threat analysis, and incident response.
Security monitoring and event analysis	Identify indicators that show an incident has occurred and initiate swift response, differentiating between those incidents that represent impotent attack vectors and those that need to be analyzed in-depth by the incident responders. Many other tasks are performed by the security monitoring and event analysis staff, but the ones described here are the critical tasks for which skills are in very short supply.	Failure to identify new attacks that mimic old, impotent attack vectors provides savvy intruders with an easy vector to bypass defenses.
Incident responder in-depth	Implement proactive measures to contain the incident, including isolation, characterization, reverse engineering, assessment of capability and activity of malicious software that has been found on agency systems, identification of intruder local changes/suspect interactions, triggering of targets to evoke malicious behaviors, and development and deployment of eradication tools. Only 2%–10% of all malicious software needs to be put through this deep analysis; the remainder will be cleaned with anti-virus tools using current and updated signatures. However, the 2%–10% constitute the most dangerous payloads.	Malicious software will be able to spread through agency systems by burrowing deep and maintaining control as well as by leaving back doors for unauthorized access at will. An unacceptable duration of attacker free time will result in freedom of movement and action. Lack of understanding of attackers and their tools (advanced malware) will undercut the defensive efforts of incident responders and threat analyst. Attackers can reuse tactics and tools to re-attack or maintain their control over systems for long periods, taking and changing data at will. Anomalous and malicious behavior by insiders will go undetected.
Threat analyst/ Counter-	Deploy deep and current knowledge of the attack surface, its most vulnerable and high value targets, and how its technical vulnerabilities may	Malicious software installed by targeted attacks and other vectors will be able to evade defenses without being spotted—leading to long-term infection,

intelligence analyst	be exploited; maintain up to the minute situational awareness on what malicious actors are using and targeting; and develop techniques and program custom tools to detect local changes, identify suspect interactions, and watch for and respond to what the malicious actors are doing. More advanced teams also are able to understand the attackers' motivation, language, organization, and social behaviors, as well as group the threat actors logically to create effective "cyber" profiles of groups, actors, and campaigns, thereby helping organizations become more proactive in their security posture and defense.	freedom of action (including the exfiltration of sensitive information), and undermining of the defender's ability to act. Well-embedded adversaries can actually resist defender efforts as they are privy to instructions and can work to stay a step ahead of observed defender actions. Further, not understanding the current threat landscape and exactly how the attacks work in technical detail will lead to insufficient defenses against those vectors and will unnecessarily raise costs.
Risk assessment engineers	Develop estimates of the risks associated with deployment of new technologies and of newly discovered threats, enabling businesses and agencies to assess the resources needed to respond effectively.	When this is done incorrectly, resources are allocated to the wrong tasks and to deploy the wrong tools. Doing this task well requires significant hands-on technical expertise to assess how the threats will manifest and how defenses will need to be deployed and/or altered.
Advanced forensics analysts for law enforcement	In investigating crimes or potential crimes, the advanced forensics analyst must perform many of the tasks of the incident responder in depth, with special emphasis on reverse engineering but with the added requirement of establishing evidence that will stand up in court. Responsibilities include: determining programs that have been executed, finding the files that have been changed by an intruder on disk and in memory, using time stamps to develop authoritative timelines of actions taken by the intruder, finding evidence of deleted files, and identifying key information in browser histories, account usage, and USB usage. The central goal is to find unknown malware hidden in systems, also known as the persistent presence.	Too few forensics analysts have the deep technical skills to go beyond the most basic capabilities of the common commercial forensics tools. The FBI reports that nearly every case now involves computers; lack of deep forensics skills can render law enforcement agents impotent. DHS, in partnership with law enforcement, can add value to industry by providing tools and expertise, thereby reducing industry costs during incident response and investigation.
Secure coders and code reviewers	Write code free of known coding flaws and weak design approaches, and check software to find flaws and fix flaws that are found. The most proficient are those coders who possess the cognitive capacity to discover security vulnerabilities in programs while under time, quality, or cost pressures (i.e., the real world).	Intruders and malware exploit flaws to: modify, add, or delete code on web sites that infect visitors' computers, deeply embarrassing the agency; or leverage their modifications as access pathways for data exfiltration.
Security engineers-operations	Implement and configure host and network firewalls, logging, and IPS/IDS at the highest appropriate level of security, and implement automated monitoring of configuration, patching, AV status, administrative rights, application white listing, and other security measures in order to give system and network administrators daily actions to maintain the highest possible level of security and to ensure that those actions are being performed.	The most common forms of targeted intrusions easily penetrate the defenses. Cybersecurity engineers are the main defense in power companies and other critical infrastructure enterprises. Without a team of cybersecurity engineers that can match the capabilities in industry, DHS will have trouble partnering with industry in the critical infrastructure.
Security engineers/ architects for building security in	Maintain up-to-the-minute currency on attack techniques being used by adversaries against any of the components being engineered into new or updated systems. Avoid myths about design controls that are considered to be effective but, in fact, are not. Use knowledge about current attacks to identify flaws and weaknesses in the composition and design of networks, remote	When security is not baked into systems at the outset, it is very hard to glue it on later.

	access schemes, and systems and applications. Specify solutions and verify the solutions that have been implemented. Rapidly adjust designs based on new threat and attack information.	

Recommendation 1: Question/Answer

Question: The National Initiative for Cybersecurity Education (NICE) Framework already covers these jobs and skills. How does implementation of this recommendation take advantage of the work done in developing the NICE Framework?

Answer: NICE is a comprehensive catalog that lists hundreds of tasks and skills, organized by categories and specialty areas. NICE's Background Paper says that "all cybersecurity work can be described using the Framework."[19] To take full advantage of the NICE framework, DHS must define and differentiate specific jobs and skills that are mission-critical for DHS-specific mission sets. Implementing this recommendation will make the NICE framework more valuable for hiring managers at DHS (and at many other organizations) by clarifying those functional roles within the framework that are mission-critical and by defining DHS-specific job requirements that can then be prioritized and binned into mission-critical and non-mission-critical categories. The national program manager for NICE at the National Institute of Standards and Technology, Dr. Ernest McDuffie, encouraged the Task Force to take on the specific adaptation of the NICE framework for mission-critical roles, expressing the sentiment that it was "much needed."[20]

Recommendation 2: Develop training scenarios that enable evaluation of mission-critical cybersecurity talent for each of the mission-critical tasks shown in Table 1.

Mission-based training scenarios help develop and measure proficiency in performing mission-critical tasks. This approach of identifying scenarios and requisite actions and skills is commonly used in assessing and rating job skills in many professions—particularly where lives are at stake.[21] Since 2011, the U.S. Department of Energy has been developing scenarios to tease out job performance models and establish methods to assess competence in mission-critical cybersecurity roles in the power industry. Power industry leaders who have used the resulting assessment methods say this marks the first time they have fully understood the tasks and skills needed to respond effectively to the cybersecurity manpower challenge.[22]

The Department of Defense (DoD) has also demonstrated that it recognizes the value of scenario-based training and assessment in cybersecurity. In August 2012, DoD issued a request for researchers to "build a system that can replay cyber attacks" in order to "enhance training and cyber situational awareness" for its cybersecurity workforce.[23]

To implement this recommendation, the Department should:

- Build on the Department of Energy's effort to develop mission scenarios, requisite cybersecurity skills, and rating methods to take advantage of common scenarios

and lessons learned, and to accelerate the establishment of a similar structure for DHS.
- Allocate 90 days for a review and update of the Department of Energy structure. At the end of that review, begin implementing the resulting structure.
- Establish a panel of cybersecurity practitioners to update and maintain the structure on a periodic basis.

Recommendation 2: Question/Answer

Question: How much time and resources does it take to develop the complete analysis?

Answer: Teams performing similar scenarios and rating systems on behalf of the Department of Energy found that they can complete the needed tasks in approximately 90 days per skill area.

Recommendation 3: Adopt a sustainable model for assessing the competency and progress of the existing and future DHS mission-critical cybersecurity workforce.

To implement this recommendation, the Department should:

- Establish a certification program for each mission-critical job using simulation-based proficiency evaluation combined with written examinations to verify competency.
- Require employees to update their certifications at least every two years.
- Rely on objective and measurable performance standards for the various mission-critical roles established in implementing Recommendation 2.

The Task Force considered several proficiency testing models, including those used in evaluating physicians, pilots, and attorneys and found that the Federal Aviation Administration (FAA) model for training and certifying pilots provided a promising approach. As in cybersecurity, pilots may specialize in many different types of aircraft, with each type requiring separate proficiency assessment and ratings. Physicians also have many specialties; the live "board certification" process used in medical specialty areas for nearly a century is envisioned as the model for scenario-based proficiency measurement for cybersecurity specialists. Lawyers on the other hand, generally pass only a single bar exam and specialists are not separately assessed.

Pilot assessment is rigorous, reflects technical skills with many nuances, is repeated often, and does not necessarily require seven to 10 years or more of collegiate and post-graduate training, as is required for law and medicine. Pilot training employs operational scenarios to create a realistic context for teaching specific skills and evaluating performance in executing a wide range of tasks.[24] As proficiency improves, conditions are made more difficult to induce stress. For example, deteriorating weather and system malfunctions are added, and emergency conditions created. The result is a continuous improvement in pilot competency and proficiency.

The key for aviation—and the key takeaway for applying the same approach to training for mission-critical cybersecurity professionals—has been setting the pilot certification standards at the appropriate level, and then enforcing those standards vigorously using recurrent scenario-based training and evaluation.

Objective 2: Help DHS employees develop and maintain advanced technical cybersecurity skills and render their working environment so supportive that qualified candidates will prefer to work at DHS.

The Challenge: Enable DHS to build a large, highly technical cybersecurity workforce from a very small base. Table 2 shows the challenge DHS faces in competing for technical talent against organizations with stronger technical teams and reputations. DHS needs to provide structural support for the most talented technical people so that their skills can stay current and so they will want to come to DHS and, once they are there, will want to stay.

Table 2: Where Scholarship for Service (SFS) Graduates Have Gone to Work, 2002-2012[25]

Agency	SFS Graduates Hired	Percent of Total
Total	1,076	
National Security Agency	349	32%
Navy	99	9%
Army	55	5%
Mitre Corp	45	4%
CIA	37	3%
Sandia Laboratory	35	3%
Air Force	33	3%
Government Accountability Office	33	3%
Defense Information Systems Agency	32	3%
Federal Reserve	28	3%
Department of Homeland Security	*25*	*3%*
Army, Software Engineering Institute	18	2%
Department of Justice CIO	18	2%
FBI	16	1%

Recommendation 4: Establish a Department-level infrastructure with direct responsibility for the development and oversight of the cybersecurity workforce.

A new infrastructure must be established using five mechanisms to enable DHS to provide a supportive environment for technical cybersecurity professionals: (1) eliminate unnecessary delays in hiring and promoting technical cybersecurity professionals; (2) bring a total-organization perspective to personnel actions (selection, training, development, placement, and compensation); (3) directly involve the existing top technical talent to guide the development of others; (4) establish full career-track patterns and growth; and (5) create buy-in and investment by line organizations.

To implement this recommendation, the Department should:

- Establish a centralized, Department-wide "Cyberworkforce Board" with two sets of responsibilities:
  - Set strategic targets for workforce development; establish targets for the federal/contractor mix; put in place workforce development priorities; establish career paths; and provide Department-wide advocacy for cybersecurity career fields. This Board would also advocate for and manage special programs for additional compensation, bonuses, and awards directed at mission-critical jobs and people.
  - Establish relevant criteria, standards, and career paths; regularly reexamine skill needs, build these needs into development programs, and feed that

information back into hiring and assessment processes; ensure alignment of human resources and supporting infrastructure; and provide mentoring.

- Establish a standing external (e.g., academia, research, industry) "Cyberworkforce Advisory Board" to advise on cybersecurity workforce issues.
- Examine and manage the mix and placement of political versus federal civilian executive positions in cybersecurity, with a focus on ensuring continuity.
- Establish employee-led improvement programs for cybersecurity professionals with leadership-supported mechanisms to identify areas of improvement, take action, and ensure accountability.
- Focus increased attention on establishing information opportunities for cybersecurity employees at DHS like town halls, surveys for feedback, "brownbag events," and access to executive leaders.
- Use a "talent judging talent" model that directly involves the best of the current cybersecurity workforce to define the needed skills, train and mentor, and recommend new opportunities.
- Establish and manage cross-Department, skill-based structures (e.g., Air Force Career programs, industry career path models, National Security Agency Skill Communities) to oversee many of the activities listed above.

The approach of managing a community with a department-level infrastructure is common in large organizations and has been used successfully in government and industry, in cyber-related careers, and in other career fields such as acquisition.

For example, both DHS and the Air Force have developed Acquisition Career Programs for civilian employees working in the acquisition arena. The career program helps acquisition professionals manage their careers by providing career progression patterns, focused training/education (e.g., short courses as well as opportunities for advanced degrees), and development opportunities such as career-broadening assignments both within and outside DHS and the Air Force acquisition organizations. The Acquisition Career Program at the Air Force is managed by a Policy Council of appointed SES-level individuals from across the Air Force acquisition community. The Policy Council establishes the target career progression models, defines position qualification standards, oversees spending of central funding for development and training of civilian acquisition professionals, and establishes policies for civilian acquisition professionals (the people) and acquisition positions (the jobs). An example policy is that all acquisition positions in GS-14 and GS-15 levels are filled only from among Acquisition Career Program members. The Acquisition Policy Council also has a budget for hiring interns who are graduates from top schools who will be placed in an accelerated development program with accelerated promotions (up to a GS-12 level).

The NSA uses a model called Skill Communities with similar attributes for disciplines like Mathematics, Information Assurance, Networking, etc. Skill Communities are extra-organizational constructs that define expected career paths, training requirements, and applicable professional standards for professionals in the Community. They typically have an executive-level (SES) Senior Advocate, some sort of volunteer governing board of mid-to-senior practitioners, and an associated Intern Program. They are led by people from multiple

line organizations, but with significant full-time support from the in-house school and Human Resources.

The key to success is that these kinds of actions must be driven by technical people and by line organizations, with support from the human resources system. This ownership is essential, and provides a means and incentive for senior technical leaders and managers to think and act beyond their local interests.

Recommendation 5: Make the hiring process smooth and supportive and make mission-critical cybersecurity jobs for the federal civilian workforce enticing in every dimension: in mission and service, skills, growth potential, and "total value proposition."

Given the competitive marketplace, and the constraints on federal employment, the Department's competitive edge in hiring and retention is in the jobs themselves. People are much more likely to stay in federal service if they feel that they are doing unique work and have unique opportunities, are in service to something bigger than themselves, and believe that the people and the system they work for care about their long-term careers. This kind of action must be managed and "branded" by assigning a senior executive to drive it. But first the Department must improve its hiring process through the following steps:

1. Create and maintain a set of standard position descriptions to use for roles in which the mission-critical tasks in Table 1 are performed, at various classifications, to eliminate most delays associated with developing unique position descriptions.
2. Establish career ladder positions to enable noncompetitive promotion of individuals to a higher grade without further competition.
3. Use open announcements for mission-critical jobs.
4. Use IT Specialist 2210 (Security) noncompetitive selection and Schedule A appointments, with OPM approval.
5. Place steps 1-4 under the authority of the Chair of the Cyberworkforce Board.

In addition, Congress should grant the Department human capital flexibilities in making salary, hiring, promotion and separation decisions identical to those used by the National Security Agency for hiring and managing its cybersecurity workforce and other technical experts.

The actions that the Department should take to ensure jobs at DHS are enticing include the following:

- Ensure that many of the most technically-demanding jobs, such as penetration testing and incident response, are reserved for federal employees, guaranteeing both exciting jobs and opportunities for federal employees to develop solid technical foundations.

- Establish clear career paths of upward development, responsibility, and mobility, including programs such as Senior Scientist, Technical Director, etc.—in other words, the concept of "careers, not jobs."
- Focus more attention and resources on marketing the DHS-level "branding" of cybersecurity positions, including elements such as: "cool jobs" that are particularly challenging and stimulating; national service; direct partnership across the entire government; and unique access to senior decision makers and technical leaders across industry, academia, and the research community. Plan the campaign of external branding through outreach such as a "Cybersecurity Experts Speaker's Bureau," public appearances, publications, and building on the current work of the DHS Office of Academic Engagement to establish an Academic Speaker Series.
- Provide access to interesting and unique workspaces with tools, laboratories, and test environments that will promote growth of skills.
- Establish, manage, and advertise a "total value proposition" of compensation that bundles all of the elements above.
- Starting from the existing Centers of Academic Excellence in Information Assurance Program, focus on the schools that are producing the highest number of graduates with advanced technical skills in order to maximize the use of scarce technical resources at DHS; build working relationships with line organizations by assigning a single senior technical expert (DHS Liaison) to oversee the DHS relationship with each target school. Empower the DHS Liaison with the authority to offer the school sponsored research tasks, technical visits, guest lecturers, faculty exchanges, and sabbatical programs. As the number of technically sophisticated federal employees grows, the number of partner schools can grow as well.

In the list above, the Task Force suggests promoting DHS's total value proposition, a powerful notion for federal service. People who enter or stay in public service, especially in technology fields, are generally not expecting the largest salary. They are often driven by the notion of service itself, and the opportunity to do something unique. If you want the best people to stay, you also have to have the best jobs to attract them—"cool jobs" that are exciting, challenging, and offer a path of growth in skill and responsibility. Explicitly defining and managing the total value of a federal career provides the best opportunity to attract and retain the best talent for federal service.

Also in the list, we recommend more emphasis on branding. Branding can establish public recognition, build pride and ownership in the current workforce, and turn every "touch" into a recruiting and public relations opportunity. It requires creating and delivering a consistent and positive message through a planned series of engagements. The biggest challenge is to create and deliver the message at multiple levels of line organization, not simply to produce slogans, brochures, and advertisements.

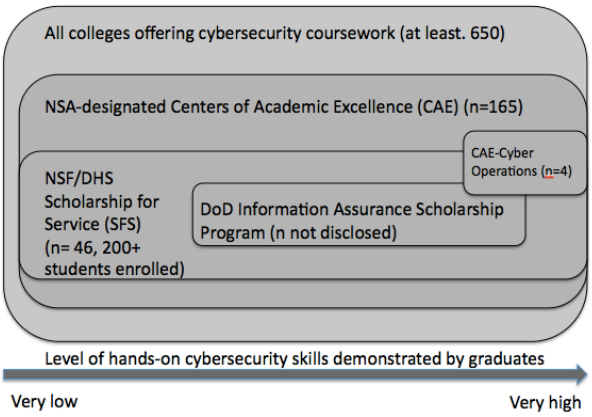
Objective 3: Radically expand the pipeline of highly qualified candidates for technical mission-critical jobs through innovative partnerships with universities, community colleges, organizers of cyber competitions, and other federal agencies.

Through innovative partnerships with universities, community colleges, the military, and organizers of cyber competitions, as well as with other federal agencies tasked with expanding job programs, DHS can ensure that a sufficient pipeline of qualified cybersecurity people is being developed and that a sufficient number of those people also gain security clearances so they can be ready to serve quickly.

DHS must improve its ability to compete with other employers in hiring technically talented graduates from the Scholarship for Service (SFS) Program. Of the more than 1,000 SFS graduates over the past 10 years, DHS hired only 25 (see Table 2). Recommendations 4 and 5 will help DHS compete for the top technical talent by fostering a work environment that the technically talented want to join (e.g., "cool" jobs, talented peers, and mentors) and then utilizing this technical talent to more successfully recruit.

The SFS is one of three national scholarship and recognition programs sponsored by the U.S. government to highlight and encourage intensive cybersecurity education in colleges. The others are the Information Assurance Scholarship Program (IASP), administered by the NSA, where graduates take on obligations to work for the Department of Defense or for an intelligence agency after graduation, and the more widely known National Centers of Academic Excellence (CAE) in Information Assurance, sponsored by DHS and the NSA. The CAE program does not offer scholarships but CAE designations are highly sought after by schools that use "an NSA-designated Center of Academic Excellence" in their promotional literature and radio advertising when recruiting students.[26]

Fig 1. Selected Federally-sponsored collegiate programs in cybersecurity*



*Sources: (1) Colleges offering degrees in CIP Code 11.1003, "Computer and Information Systems Security" 2009-2010, IPEDS data from US Department of Education; (2) NSA website on the National Centers of Academic Excellence program, and the (3) National Science Foundation Scholarship for Service Program Manager.

CAE designations are also required or highly recommended for schools attempting to win federal funding to give scholarships under either SFS or IASP. Figure 1 shows the size of each of these programs as well as the level of hands-on cybersecurity skills demonstrated by their graduates. CAE schools vary widely in the level of hands-on technical proficiency of their faculty and the students they produce. SFS schools show nearly the same level of variability in the technical proficiency of graduates. Only the CAE-Cyber Operations schools assure employers that hands-on skills are a major criterion for graduation.

Even with increased funding, SFS will graduate only a few hundred people a year going forward – not nearly enough for DHS to win the numbers needed for a rapid build-up of its mission-critical cybersecurity work force. The Task Force anticipates that implementing

Recommendations 6-8 under this objective will rapidly increase the number of graduates with advanced cybersecurity skills and allow DHS to recruit a sufficient number of technically talented cybersecurity employees.

Recommendation 6: Establish a two-year, community-college-based program that identifies and trains large numbers of talented men and women to prepare them for mission-critical jobs in cybersecurity.

In implementing this recommendation DHS will:

- Establish 10 pilot programs at community colleges, modeled on military education programs that graduate the most technically skilled cybersecurity professionals and on CAE-Cyber Operations and other academic programs where graduates have deep hands-on skills developed in real-world projects. Expand the number of programs, with a goal of establishing 50 programs across the nation as the curriculum matures and the pilot programs demonstrate success.
- Partner with the Department of Veterans Affairs and Department of Labor to synchronize these pilot programs with national manpower development priorities.
- Focus eligibility for the program on graduating high school seniors, the long-term unemployed, veterans, and men and women seeking a second career.
- Establish entry qualifications that rely on cyber competitions and games or tests to evaluate relevant foundational skills and knowledge, in order to ensure the students entering the program have a high probability of succeeding.
- Approve programs comprised almost entirely of courses with hands-on components and frequent testing that ensure actual mastery of the knowledge and skills.
- Choose or develop certification programs, based on the certification programs identified in Recommendation 3 on page 10, that measure sequential mastery of foundational and more advanced cybersecurity skills so students and employers can judge their progress based on becoming certified.
- Include a residency program that enables the most successful students to work on real-world cybersecurity projects, using projects supplied by DHS (US-CERT, U.S. Secret Service, Immigration and Customs Enforcement) and by government and private enterprises. The residents will be paid for their work and may be eligible to earn security clearances even before finishing the residency program.

Community colleges offer a fertile platform for rapidly developing a large number of highly skilled cybersecurity professionals. Four-year degrees and even graduate degrees may be of great value in preparing people for some roles in cybersecurity, but many people currently doing advanced cybersecurity tasks—from reverse engineering to application penetration testing and security engineering and architecture—learned their security skills on the job. Many military veterans develop these skills in high-tempo operational environments. One survey showed 24% of active cybersecurity professionals had no college degree.[27] Indeed, today's high school students are tech savvy and highly skilled, as the case study in Box 1 shows.

Box 1: Northrop Grumman and Lockheed Martin Internship Programs

Northrop Grumman's CyberCELL and Lockheed Martin's Chief Technology Office internship programs foster the professional development of high school and college interns, encouraging passion for science, technology, engineering, and math.

Over the course of their eight-week internship, Northrop Grumman's 2012 CyberCELL interns design and develop a complex cyber combat modeling and simulation tool, which spans the full system development lifecycle. Starting with the operational hard problem of modeling and simulating the cyber battlespace, interns define requirements and develop use cases, activity diagrams, and sequence diagrams. The interns then implement over 20,000 lines of Java code with 650 check-ins, concluding with sell-off of their final product to both mentors and Northrop Grumman executive leadership in a capstone presentation.

Lockheed Martin's interns are integrated into product line development and engineering teams to work on "real life" complex problems. The 2012 cyber interns architected a secure Geo Location application, based on the Android platform, which could provide and accept telemetry in a secure and safe manner to enable battlespace awareness and resource deployment. The team created a prototype consisting of 10 to 20 external libraries and an application programming interface. Using secure but agile processes, the interns developed and integrated over 15,000 lines of code and reviewed all code for security vulnerabilities. The interns presented their solution to Lockheed Martin's senior technical and business development leadership during a Lockheed Martin innovation forum. Their accomplishment was remarkable, as some interns had never coded or implemented security in the

Students who successfully complete these community college-based cybersecurity programs will be highly sought after. It is quite likely that they will be able to gain employment in organizations that have tuition reimbursement plans so they can complete four-year and even advanced degrees while working in the field, if they so choose.

Partners: The U.S. Department of Labor and the U.S. Department of Veterans Affairs both have programs that are highly complementary, making them effective partners with DHS in launching the community college program. For example, the Labor Department has a program that provides funds to community colleges to expand and improve their ability to deliver education and career training programs that can be completed in two years or less and prepare program participants for employment in high-wage, high-skill occupations. Similarly, the Department of Veterans Affairs offers multiple tuition reimbursement programs, some including stipends for living expenses, for veterans who seek to develop the skills needed to gain employment.

Intense courses: The community college programs will be comprised of intense courses and frequent testing. Courses will deliver practical, hands-training similar to that used to impart

technical cybersecurity mastery to military and law enforcement professionals and to technical security professionals at banks and other enterprises where security is a high priority. These courses will range from basic content on the fundamentals of cybersecurity (basic networking, operating systems, and system administration) to more advanced topics such as perimeter protection, secure coding, advanced forensics, hacker techniques, incident handling, mobile security, system and application penetration testing, and reverse engineering. The list of recommended courses will be updated by the DHS Cyberworkforce Board as needed to reflect new threats and technology. Using certificates rather than degrees as proof of completion will allow community colleges to launch the pilot programs without long delays.

For schools that do not yet have faculty with the hands-on skills to teach the intense courses, teachers may be adjunct faculty from local employers who want to establish pipelines of skilled professionals. Alternatively, community colleges may gain economies of scale by using online programs to deliver expert teaching and inviting local employers to supply staff who help the students master the hands-on exercises in lab sessions.

Residency Program and DHS: The residency programs will rely on work from many employers, but it is essential that DHS provide a substantial amount of that work and that DHS technical staff work closely with the schools to serve as role models and to build long-term relationships that can lead to the best and brightest students joining DHS.

Recommendation 6 Question/Answer:

Question: What if the community colleges want to focus on other aspects of cybersecurity, such as policy and compliance topics?

Answer: Nothing would prevent them from doing so, but the Task Force found that the national security imperative arising from the current shortage of hands-on technical skills is sufficient to warrant focusing the entire DHS-sponsored community college program on hands-on, advanced mission-critical cybersecurity skills.

Recommendation 7: Raise the eligibility criteria for designation as CAE and SFS schools to ensure that graduates are prepared to perform technical mission-critical cybersecurity jobs.

Although it may appear counterintuitive, raising the standards for inclusion in the CAE and SFS programs is more likely to increase rather than decrease the number of people with hands-on skills graduating from those programs. The reason for this is that too many graduates from CAE schools have not had sufficient hands-on experience or sufficiently expert guidance to make them valuable in mission-critical cybersecurity jobs. Raising the bar will encourage schools to upgrade their programs.

To implement this recommendation, DHS should:

- Create a new CAE-Cyber Defense program using the approach developed for the National Centers of Academic Excellence in Cyber Operations (CAE-Cyber

Operations) and focus that approach on computer network defense, including secure provisioning of new systems and secure operations of existing systems.
- Rank colleges in the CAE and SFS program on the number of people they graduate each year who are proficient in each of the mission-critical cybersecurity skills.

We have found evidence that raising the bar for qualification accelerates program improvement and growth. NSA built a new higher standard inside the CAE program called CAE-Cyber Operations. Four schools reached the higher standard and were accepted; several schools that did not qualify in 2012 are working diligently to improve their programs of instruction so they can be eligible in 2013. Box 2 shows how it was done.

Box 2: The CAE-Cyber Operations Program

To create the CAE–Cyber Operations requirements, a National Security Agency team composed of people with hands-on knowledge of how to perform the key tasks associated with cyber operations identified the skills that college graduates and other incoming personnel needed in order to be fully functional in a few weeks, instead of after a long period of remedial training. Then the NSA team fit the needed knowledge and skills into specific courses often offered at colleges and outlined the specific topics those courses needed to include. Most importantly, for each course, the team specified the measure of mastery that would demonstrate that students had learned the essential knowledge and skills. For a software analysis course, for example, the expected outcome is *"Students will be able to perform analysis of existing source code for functional correctness. Students will also be able to apply industry standard tools that analyze software for security vulnerabilities. Through the application of testing methodologies, students should be able to build test cases that demonstrate the existence of vulnerabilities."*

The improved requirements included core and optional courses so students can specialize in areas of cybersecurity operations of interest to them. The colleges develop the courses, but the NSA criteria establish what the students need to know and be able to do upon completing the courses.

The NSA invited all 124 four-year CAE colleges to apply; 20 did so and four made the cut and are operating today as CAE-Cyber Operations schools. Their students and faculty attend special programs at NSA and work on NSA-sponsored projects, during which time students also undergo security clearances. Faculty members at those schools laud the program for helping them ensure that their students are being extremely well prepared for some of the hardest jobs in security. Importantly, the sponsors at NSA agree.

Recommendation 7: Question/Answer

Question: If a CAE school cannot enhance its programs to become eligible for the CAE-Cyber Defense designation, will it be able to remain in the CAE Information Assurance Program?

Answer: The national shortage of professionals with mission-critical skills, combined with the surfeit of people who are employed in cybersecurity without the requisite skills to perform mission-critical tasks, leads to the conclusion that no federal recognition should be given to schools unable to produce mission-critical talent. Allowing other schools to retain the "center of excellence" designation would confuse students and possibly cause them to earn degrees for jobs that are not likely to exist. However, the transition should not be abrupt. Current CAE-designated schools should be afforded two years to make the transition.

Recommendation 8: Launch a major, sustained initiative to enhance the opportunities for U.S. veterans to be trained for and hired in mission-critical cybersecurity jobs.

The United States owes a great debt to its veterans. At the same time, America's veterans represent a unique pool of candidates with proven talent and a proven commitment to public service. Programs are already in place (federal, state, academic, and private sector) for job training and tuition support, job counseling and placement, etc. However, these programs have not been able to target mission-critical cybersecurity jobs effectively, because they have not had access to federal cybersecurity professionals in a position to help them target their programs to the most important areas where the best jobs are located. DHS can help the nation build its cyber manpower pipeline and help veterans at the same time by investing heavily in partnering with and supporting the sponsors and recipients of national, large-scale jobs programs.

To implement this recommendation, the Department should:

- Sponsor a national competition, with significant promotion by DHS and other national leaders, including military and intelligence leaders, to encourage and enable veterans to qualify for places in the community college program implemented in Recommendation 6.
- Establish a classified residency program, exclusively for veterans, so those who have completed the community college program can earn security clearances and work on classified cybersecurity projects as part of their training.
- Develop a mentoring program in which veterans who have won cybersecurity jobs mentor other veterans who are attempting to enter and who are progressing through hands-on cybersecurity training programs.
- Provide wounded warriors with additional support as needed.
- Develop a web page, mirrored at both DHS and the Department of Veterans Affairs (VA) web sites specifically for veterans showing how to use the VA benefits programs such as Post-9/11 GI Bill and/or VRAP to gain entry into mission-critical cybersecurity careers. Include video interviews on the site of veterans who hold cool jobs in cybersecurity and include roadmaps showing veterans the pathways available in the cybersecurity field.
- Establish entry qualifications that rely on cyber competitions and games or tests to improve the probability that veterans will succeed when they enter the intense hands-on cybersecurity training programs.
- Choose or develop certification programs that measure sequential mastery of foundational and more advanced cybersecurity skills so veterans and employers can judge their progress based on becoming certified.
- Partner with the Department of Labor (DoL) to jointly establish at least 25 DoL community college programs, in areas of the country where large numbers of veterans live, designed exclusively for veterans who have been unemployed or are looking for a second career.

Objective 4: Focus the large majority of DHS's near-term efforts in cybersecurity hiring, staffing, training, and human capital development on ensuring that the Department builds a team of approximately 600 federal employees with mission-critical cybersecurity skills.

The recommendations under the previous objectives provide the means to radically increase the number of people with mission-critical skills to be produced by academic institutions each year and to make DHS a desirable and exciting employer for highly talented technical cybersecurity professionals. Implementing the recommendations under this objective will ensure that DHS actually hires the people with those technical mission-critical cybersecurity skills.

In order to accomplish this objective, DHS will need to retool current recruiting practices for mission-critical cybersecurity roles, commit sufficient staff to compress selection process timelines, and intensify targeted training opportunities to maximize the capabilities of the cybersecurity workforce. As these efforts to develop a federal staff are underway, DHS should upgrade the technical skills of contract personnel deployed to fill mission-critical roles.

Recommendation 9: Until 600 employees are on board with mission-critical cybersecurity skills, apply the large majority of direct hire and excepted service authority related to information technology in DHS to bringing on people with technical mission-critical cybersecurity skills as demonstrated in tests using the scenarios and rating system developed in implementing Recommendations 2 and 3. Focus schedule A/2210 hires on those with mission-critical skills.

To implement this recommendation DHS should:

- Facilitate a rapid expansion of the mission-critical-capable staff by having the Deputy Undersecretary for Management and the Chief Financial Officer of DHS reprogram funds so that at least 50 mission-critical ("cool") positions now filled by contractors will be filled by newly hired federal employees within six months.
- Prioritize testing of all Schedule A/2210 hires with less than one year of government service, separating from service those unable to demonstrate proficiency.
- Reassign Schedule A/2210 hires beyond the probationary period to non-mission-critical information technology positions if they do not meet proficiency requirements.
- Request that the U.S. Office of Personnel Management (OPM) extend the Schedule A Excepted Service hiring authority for three more years.

DHS must lead by example if it wants to be the national leader on cybersecurity that provides specific guidance and support to other civilian federal agencies and to companies comprising the critical infrastructure. DHS cannot expect any other agency or critical infrastructure company to pay attention to its guidance if the Department does not perform mission-critical jobs at world-class levels. Top-quality technical skill will give DHS the leadership role for civil government and industry just as technically skilled cybersecurity people gave NSA the cybersecurity lead for all of DoD.

DHS has two been using two noncompetitive hiring authorities when hiring cybersecurity personnel. Schedule A hiring authority was granted by the OPM on September 21, 2009 to staff up to 1,000 positions within the cybersecurity workforce at the General Schedule (GS) grade levels 09-15. The duties for the targeted positions include such tasks as incident handling and malware/vulnerability analysis, distributed control system security, cyber incident response, vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, and investigation and investigative analysis. Unfortunately this authority expires December 31, 2012. The second authority is the 2210 Direct Hiring Authority (DHA). In 2003, the OPM established government-wide DHA for Information Technology Management (Information Security) positions in the 2210 occupational series at the GS-09 grade level and above. This authority is continuing.

Those who have been hired under the Schedule A and 2210 authorities and are still in the one-year probationary period should be tested for skill proficiency according to the job requirements. If they do not meet expected skill levels the Department has two options: assign them to other roles that do not require high-proficiency technical skills, or separate them from service. Those who are past their probationary period should also undergo testing to determine if reassignment or additional training are necessary to meet the required skill levels.

Recommendation 10: Specify the mission-critical skills and level of proficiency DHS needs in all cybersecurity-related contracting activities including RFIs, RFPs, task orders, and CRAD documentation.

To implement this recommendation, DHS should:

- Use the descriptions in Table 1 as a model for the contracting of mission-critical cybersecurity skills.
- Establish standard labor categories for the technical mission-critical roles.

Currently the DHS contracting process does not adequately specify the skills that contractors must provide the Department. This is partly due to a lack of clearly defined job categories and the critical skills needed to fulfill them. This lack of clarity leads to a skill mismatch between the skills needed and the skills available. DHS can correct this problem by making the needed skills explicit and mandatory based on the conclusions of its review.

Contractors with the right skill mix will enable DHS to upgrade its capabilities quickly. This will also allow skilled people to get a taste of the interesting work DHS does and the great team they may be enticed to join. Contractors have been hiring the best and brightest federal and civilian employees for years, and this added specificity will better align the department's needs with the skills available through contractors.

Objective 5: Establish a "CyberReserve" program to ensure a cadre of technically proficient cybersecurity professionals can be called upon if and when the nation faces a major cyber crisis.

The Challenge: Ensure that talent developed at DHS remains available to the Department in times of need and that additional talented cybersecurity professionals are available to supplement federal manpower in times of great need.

Recommendation 11: Establish a pilot DHS CyberReserve program that ensures DHS cyber alumni and other talented cybersecurity experts outside of government are known and available to DHS in times of need and determine how this program may be implemented over the long term.

To implement this recommendation, DHS should:

- Develop a voluntary skills proficiency and mastery inventory, using the jobs and skills identified in Table 1. Add industry-specific mastery including SCADA systems expertise in each mission-critical job. To provide more effective localized cybersecurity support to critical infrastructure and law enforcement, encourage the U.S. Secret Service's Electronic Crimes Task Forces (ECTFs), as well as other appropriate local groups, to participate in the skills inventory.
- Establish a 90-day working group to explore key questions concerning the feasibility and workings of a CyberReserve program that offers exclusive access to key threat information, defensive tactics, and security clearances in return for a contractual agreement to provide assistance to the government when the Secretary of DHS calls upon them.

The Skills Proficiency and Mastery Inventory

Box 3: Electronic Crimes Task Forces

Located in 25 metropolitan areas, ECTFs bring together not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. ECTFs have experience building relationships among their local partners to improve response to cyber incidents. Further, ECTFs already serve as a forum for government agencies such as DHS, NSA, and the Departments of Justice and Treasury to provide sensitive briefings to select members and representatives from a specific business sector. ECTFs' membership databases could easily be adapted to include skills inventory information.

DHS should develop a protected database containing its direct knowledge about skill levels of people in government and in contractor organizations who have basic proficiency and who have mastery in each of the mission-critical skills listed in Table 1. The resulting skills inventory will allow DHS to quickly find staff and contractor personnel who can fill specific job needs. Even after the people leave DHS, the inventory may prove to be valuable in finding talent in times of emergency. The optimal value of a skills inventory may be indentifying locally available talent, which may be done best by partnering with Electronic Crimes Task Forces (ECTFs) and similar groups such as the FBI's InfraGard chapters (See Box 3 for a description of the ECTF structure).

This inventory may offer an additional benefit of strengthening partnerships between DHS and industry and providing access to the specialized skill sets needed to respond to a significant cyber incident as described in the National Cyber Incident Response Plan which says, "As key owners, operators, and leaders in cyberspace and as a key part of National Cybersecurity and Communications Integration Center operations, Critical Infrastructure/Key Resource owners and operators are likely to be called upon to assist the Federal Government during a Significant Cyber Incident."[28]

Working Group to Plan a DHS CyberReserve Program

A ready reserve of mission-critical technical talent, through which people who are trained and who serve with distinction at DHS might continue to serve their nation, is an important objective. As cyberspace is largely owned and operated by the private sector, creating a mechanism to effectively tap into the expertise resident in the private sector during a national cyber emergency is vital to recover critical infrastructures. Incident response with private industry is a slow process—government entities need to be invited into the facility, legal agreements must be reached, and assurances must be given that the people assisting are not going to seize equipment. Private asset owners are more receptive to federal assistance when those who will be responding have direct knowledge and experience with their vendors and systems. In a CyberReserve structure, many more people with industry experience will be directly available to DHS, improving both the quality and speed of government help.

There are precedents for such a program. Box 4 illustrates how "reserve" utility crews help one another when storm damage needs a quick response.

Box 4: Electric Line Crews

Electric utilities have established mutual assistance agreements with other electric utilities, sometimes with competing electric service providers, for quick response restoration after weather events. These agreements may be with a pool of resources like electric membership corporations representing many smaller cooperatives or large investor-owned utilities with similar needs that mobilize teams of line crews and technicians to assist after tropical storms (e.g., Florida Power and Light and Entergy). Resource agreements for overtime pay, work conditions, and equipment are negotiated in advance of an event. Similar agreements can be designed for CyberReserves to call on a large, diverse skill set to augment DHS staff in response to a specific cyber event. Matching the specific skills and industry base will provide a more efficient response. For the CyberReservists, gaining hands-on incident response experience will be a valuable return to their employer.

This recommendation was generated late in the Task Force's deliberations and raises substantial planning questions that we were unable to answer in time to deliver with this report. We therefore recommend that DHS establish a new working group of appropriate experts to answer the following questions and prepare a report for the Secretary, within 90 days, on whether and how to establish a CyberReserve program:

- How big should the CyberReserve be? How much will it cost to set up and maintain?
- How should a call up work in the CyberReserve program?

- What eligibility criteria should be used? Consider the proficiency levels on mission-critical skills and how those levels would be established for people who never served at DHS.
- What is the business case for the CyberReserve? That is, how often and to what extent will the CyberReserve need to be used to be cost-effective?
- How should the CyberReserve cooperate with the National Guard and Reserves?
- What training and other benefits should the Department provide members of the CyberReserve? Consider maintenance of security clearances; access to early data on promising defensive practices; training materials; and a tactics, techniques, and procedures sharing program that enables members to share the lessons they are learning in a protected environment.
- How long and under what circumstances would members maintain their eligibility?
- What communications systems will be used to contact reservists if the IP network goes down?
- What would be the contractual obligations of the reservist, the Department, and the reservist's employer?
- Under what circumstances may the Secretary call up the CyberReserves?
- How would conflicts between DHS needs and employer needs be resolved?
- How would potential conflicts of interest (e.g., if an employee of one company is called up to assist a competitor) be resolved? Should the individual decide?
- What training tools, such as modeling and simulation tools and techniques, are effective in determining cyber reserve skills necessary for an appropriate response during cyber emergencies? Should DHS establish an active research and development program to identify potential critical infrastructure cyber scenarios, determine effective responses, and plan for the skill base necessary to actively mitigate threat vectors?
- Would Congress need to grant DHS additional authorities? If so, which authorities?

Conclusion of the Task Force on CyberSkills

Our shared mission is to help protect the critical infrastructure through detecting, responding to, and ultimately preventing cyber attacks and accidents. Our deliberations identified many promising practices already underway. Much more needs to be done. The Secretary recently said that cybersecurity is the most dynamic and threatening risk we face. Her vision, that one day in the future federal agencies and private sector entities will have the technical cybersecurity workforce needed to meet their mission responsibilities, can be achieved by implementing the recommendations in this report.

[1] Gorman, S, "Electricity Grid in U.S. Penetrated by Spies," Wall Street Journal, 8 April 2009, http://online.wsj.com/article/SB123914805204099085.html.

[2] Meserve, J. Staged cyber attack reveals vulnerability in power grid. http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US; YouTube demonstration: http://www.youtube.com/watch?v=fJyWngDco3g

[3] Blakely, R, Richards, J, Rossiter, J, and Beeston, R."MI5 Alert on China's Cyberspace Spy Threat," TimesOnline, December 1, 2007 (December 11, 2007).

[4] Jarrell, D. Manager, Critical Infrastructure Protection Program, U.S. Department of Commerce, Statement for the Record, U.S. House of Representatives Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, 29 April 2007, Includes the statement "Commerce cannot clearly define the amount of time the perpetrators were inside its BIS computers before their presence was discovered." www.ogc.doc.gov/ogc/legreg/testimon/110f/jarrell0419.doc

[5] Broache, A. "Homeland Security IT chief blamed for cyberwoes," CNET News, 20 June 2007, http://news.cnet.com/Homeland-Security-IT-chief-blamed-for-cyberwoes/2100-7348_3-6192255.html?tag.

[6] Goodin, D. "Department of Homeland Security Website Hacked." Includes text: "The attack causes infected sites to redirect visitors to destinations that attempt to install malware on vulnerable machines." http://www.theregister.co.uk/2008/04/25/mass_web_attack_grows/

[7] U.S. Department of Homeland Security. "Secretary Napolitano Announces New Hiring Authority for Cybersecurity Experts," Press Release, 1 October 2009. http://www.dhs.gov/news/2009/10/01/secretary-napolitano-announces-new-hiring-authority-cybersecurity-experts

[8] Arrington, M. "Google Defense Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations," Tech Crunch, 12 January 2010, http://techcrunch.com/2010/01/12/google-china-attacks/.

[9] Clayton, M. "US Oil industry hit by cyberattacks: Was China involved?" The Christian Science Monitor, 25 January 2010, http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved.

[10] Nakashima, E. "Cyber-intruder sparks massive federal response – and debate over dealing with threats," The Washington Post, 8 December 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

[11] F-Secure presentation, May 21, 2008, IMPACT Launch at the First World CyberSecurity Summit , Kuala Lumpur, Malaysia.

[12] For example, see: McAfee Labs, *McAfee Threats Report: Second Quarter 2012*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf. Lucas, C. iSight Partners. Interview conducted August 29, 2012, Chantilly, VA.

[13] Engleman, E., Riddel, K., Holmes, A. *Raytheon, SAIC Vie With U.S. in 'Fratricide' Over Cyberworkers. Bloomberg News*, March 29, 2011. http://www.bgov.com/news_item/HMRFKLKr4Dj_sBtkxFos-Q

[14] U.S. Department of Homeland Security, Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise, November 2011, 6, http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

[15] Please see Appendix A.

[16] Due in part to the lack of common cyber job titles and descriptions and the use of contractors to both fill specific skill gaps and staff up quickly, it is challenging to determine the precise numbers of needed federal employees. With the understanding that the "right" number could be twice as large and will need to be continually reassessed as the threat picture changes, we based the target number of 600 on three sources: (1) Interviews with cybersecurity leaders in two of the largest financial companies and one of the largest technology companies who provided the Task Force with confidential counts of people currently in their organizations with the mission-critical skills in Table 1, as well as scaling information that can be used to estimate counts at DHS. The leaders also expressed a need for rapid expansion in these numbers based on the recent surge in attacks some of them are seeing. (2) The number of federal employees with advanced technical skills at the NSA's Information Assurance Division and National Threat Operation Center and at the DoD's Joint Task Force on Computer Network Operations, which together provide DoD agencies and military services with support and guidance similar to that provided by DHS to civilian agencies and critical infrastructure. (3) The number of employees hired in response to the Secretary's call for the "best cyber analysts, developers and engineers in the world" but who have not shown proficiency in the hands-on skills identified in Table 1.

[17] For example, see Federal Acquisition Regulations (FAR) Part 61 Sec 61.58 for regulations on pilot-in-command proficiency checks.

[18] The list of mission-critical skills in Table 1 was developed through an iterative, consensus-building process first involving Task Force members (including government laboratories and defense contractors) who have significant experience developing and deploying cybersecurity workforces. Subsequently the consensus group was expanded to include technical managers in commercial critical infrastructure companies (power and finance) and DHS employees with a reputation for excellence in the mission-critical skills. The list is likely to continue to evolve.

[19] National Institutes of Standards and Technology, National Cybersecurity Workforce Framework Background, Development, and Use, September 2012.

[20] Telephone interview on July 11, 2012.

[21] This technique is described as effective by the DHS Customs and Border Protection for all specialized skills, and also by the U.S. Air Force, Navy, and Army and all commercial airline companies in developing competency measures for its pilots.

[22] Reported to the Task Force at its July 19 meeting by Michael Assante, project manager for the Department of Energy's initiative in cyber skills assessment and Executive Director of the National Board of Information Security Examiners.

[23] "DoD wants system to replay cyber attacks," Federal News Radio, August 15, 2012, www.federalnewsradio.com/241/2994061/DoD-wants-system-to-replay-cyber-attacks.

[24] Lehrer, J. The Value of Simulation, Wired. June 29, 2011. http://www.wired.com/wiredscience/2011/06/the-value-of-simulation/

[25] Data provided via email by Victor Piotrowski, SFS program manager at the National Science Foundation, current as of March 15, 2012.

[26] Nearly all CAE schools use their CAE designation as a primary marketing tool. See, for example, https://www.umuc.edu/form_generator/formbuilder/index.cfm?fid=543&gclid=CLqqrr6Fm7ICFQfhQgodUV8AYg for example. It says, "The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated UMUC as a National Center of Academic Excellence in Information Assurance Education." It displays both the NSA and DHS logos.

[27] 2008 Salary and Certification Survey, The SANS Institute, July, 2008. Bethesda, MD.

[28] National Cyber Incident Response Plan, Interim Version, September 2010. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf

APPENDIX A: TASKING AND TERMS OF REFERENCE

Secretary

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 2, 2012

MEMORANDUM FOR: Judge William H. Webster
Chairman
Homeland Security Advisory Council

FROM: Secretary Napolitano

SUBJECT: Homeland Security Advisory Council Tasking

The Department is committed to ensuring cyberspace supports a secure and resilient infrastructure, enables innovation and prosperity, and protects privacy and other civil liberties by design. As you know, our goal is to protect cyberspace for the American people so our citizens can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.

Enhancing the Nation's cybersecurity requires a departmental workforce with specialized knowledge and skill. The Department must provide this workforce with clearly defined career paths, opportunities for advancement, and ongoing refinement of their skills. While DHS has devoted a variety of resources to grow its cybersecurity workforce by over 600% since 2009, more work is needed. DHS is reaching across the Federal Government, partnering with the private sector, and empowering the general public to collaborate with us in creating a safe, secure, and resilient cyberspace for the American people.

To achieve this key aspect of the Department's mission, I request the Homeland Security Advisory Council (HSAC) form a Task Force on CyberSkills. I have asked HSAC member Jeff Moss and Alan Paller, SANS Institute Director of Research, to co-chair the Task Force, whose initial recommendations should focus on the following issue areas:

1) **Best Practices:** What are some of the ongoing efforts, both domestically and abroad, to develop a national security workforce of the future? The Task Force should conduct an audit including university programs and internships, private sector programs, public private partnerships, and relevant Federal Government programs.

2) **Solving Problems via Partnerships**: How can DHS best partner with outside groups to help engage and recruit an experienced cyber workforce?

The Task Force will draw on relevant experts within the Department as necessary and present its work to the full Homeland Security Advisory Council for deliberation and discussion.

I have attached Terms of Reference that are consistent with the aims of this tasking. Should you have questions, please do not hesitate to contact Patrick McQuillan, Deputy Executive Director of the HSAC, DHS Office of Policy, at (202) 447-3409.

Attachment: Terms of Reference

HSAC Task Force on CyberSkills
Terms of Reference

- Draw on a wide range of acknowledged cyber experts, policy practitioners, and academics to identify the best ways to attract, recruit, develop, grow, and retain high quality cyber talent for the federal workforce.

- Catalogue and assess existing federal programs designed to attract, recruit, and retain cyber professionals, and identify any leading public or private programs, competitions, or degree programs which, in the Task Force's judgment, represent best in class approaches to identifying, training, and educating cyber talent. Create a framework with which to assess the competency and progress of the existing cyber workforce.

- Identify other promising public and private sources for cyber talent—including colleges, universities, competitions, private industry, not-for-profit institutions, and state, local, and tribal operations.

- Identify barriers as well as incentives that exist in the federal system for attracting and retaining high quality cyber talent.

- Outline options for federal cyber employee career advancement across the full spectrum of cyber professional opportunities—e.g., technologist, system administrator, network manager, forensic specialist, program manager, etc. Identify ways to create an environment that fosters growth and development of each member of the cyber workforce.

- How should this workforce best be managed at the federal level? On a department-by-department basis, within functional specialties across the federal workforce? Should an altogether new model be adopted to address the needs of this workforce? Rotating in and out of government? What implications will different approaches have for issues like employee benefits, performance appraisals, mobility, and career opportunity?

- Identify ways in which the Federal Government can most productively collaborate with academia as well as with the private sector to maintain a vibrant exchange of cyber expertise and talent. Identify any continuing education programs designed to keep CyberSkills current in the face of rapidly changing technologies.

- Explore ways to bridge the gap between the need to fill cyber positions rapidly with the sometimes lengthy processes associated with obtaining government security clearances.

- The Task Force should feel free to include other related issues as determined by the Department and the Homeland Security Advisory Council, in consultation with the Task Force Co-Chairs, in the course of its deliberations and formulation of recommendations.

APPENDIX B: MEMBERS OF THE TASK FORCE ON CYBERSKILLS

Homeland Security Advisory Council
Task Force on CyberSkills

Jeff Moss (Co-Chair)	Chief Security Officer Internet Corporation for Assigned Names and Numbers
Alan Paller (Co-Chair)	Director of Research SANS Institute
Steve Adegbite	Director of Cybersecurity Strategies Lockheed Martin
Asheem Chandna	General Partner Greylock Partners
Larry Cockell	Senior Vice President and Chief Security Officer Time Warner, Inc.
Robert Gallucci	President John D. and Catherine T. MacArthur Foundation
John Gilligan	President Gilligan Group
Steven Myers	Founder and Former CEO Steven Myers & Associates
Dr. Michael Papay	Vice President of Cyber Initiatives Northrop Grumman
Tony Sager	Former Chief of the Vulnerability Analysis and Operations Group National Security Agency
Nicole Seligman	President Sony Corporation of America
Michael Steed	Founder and Managing Partner Paladin Capital Group
Joe Sullivan	Chief Security Officer Facebook
Roy Vallee	Executive Chairman of the Board Avnet, Inc.
Rita Wells	Electric Sector Program Lead Idaho National Laboratory

APPENDIX C: SUBJECT MATTER EXPERTS

EXTERNAL SUBJECT MATTER EXPERTS

The following external subject matter experts provided briefs to the entire Task Force or one of its working groups. Many others experts provided individual input to Task Force members.

Mike Assante	President and CEO National Board of Information Security Examiners (NBISE)
Anish Bhimani	Managing Director and Chief Information Risk Officer JP Morgan Chase
Dr. Paul Ditullio	Deputy Chief, Air Force Testing Policy U.S. Air Force
Michele Guel	Distinguished IT Engineer and Senior Security Architect Cisco
Dr. Greg Manley	Personnel Psychologist U.S. Air Force
Dr. Ernest McDuffie	Lead for the National Initiative for Cybersecurity Education National Institute of Standards and Technology, Department of Commerce
Dr. Karen Moriarty	Senior Scientist HumRRo
CAPT Jill Newton	Chief of CNO, Cybersecurity and Information Assurance in the Associate Directorate for Education and Training National Security Agency
Dr. Josh Pauli	Associate Professor of Information Assurance Dakota State University
Dr. Victor Piotrowski	Lead Program Director, Scholarship for Service (SFS-CyberCorp ™) National Science Foundation
Scott R. 'Skip' Runyan	Technical Advisor, 39th Information Operations Squadron U.S. Air Force
Dr. Teresa Russell	Principal Staff Scientist HumRRO

Dr. Sujeet Shenoi	Professor of Computer Science University of Tulsa
Dr. Matt Trippe	Senior Scientist HumRRO
Dr. Ray Vaughn	Associate Vice President for Research Mississippi State University
Phil Venables	Managing Director and CISO Goldman Sachs
Johnny Weissmuller	Personnel Research Psychologist U.S. Air Force

DHS SUBJECT MATTER EXPERTS

The following DHS subject matter experts provided briefings to the Task Force.

Darryl Anderson	Contracting Officer Office of the Chief Procurement Officer
Charles Boyd	Branch Chief, INFOSEC Learning Development Office of the Chief Information Officer
Ed Cabrera	Assistant to the Special Agent in Charge, Cyber Operations/ ECSAP Section U.S. Secret Service
Alma Cole	Chief Systems Security Officer U.S. Customs and Border Protection
Eric Cornelius	Chief Technical Analyst ICS-CERT
Emery Csulak	Deputy Chief Information Security Officer Office of the Chief Information Officer
Chris Cummiskey	Deputy Undersecretary for Management Management Directorate
Angela Curry	Director of the National Cybersecurity Workforce Structure Strategy National Protection and Programs Directorate
David Dasher	Director of the Office of Selective Acquisitions Office of the Chief Procurement Officer

CAPT David Dermanelian	Chief Information Security Officer U.S. Coast Guard
Jeff Eisensmith	Chief Information Security Officer U.S. Immigration and Customs Enforcement
Shawn Flinn	Director of Presidential Continuity Office of the Chief Human Capital Officer
Renee Forney	Deputy Director, Balanced Workforce Strategy Program Management Office Office of the Chief Human Capital Officer
Keith Hall	Supervisory IT Specialist U.S. Citizenship and Immigration Services
Mike Jacobs	Section Chief, US-CERT National Protection and Programs Directorate
John Kappel	Deputy Director of the Indianapolis Hiring Center U.S. Customs and Border Protection
Chris Landi	Unit Chief, Computer Forensics Unit, Cyber Crimes Center U.S. Immigration and Customs Enforcement
Margaret Maxson	Director of National Cybersecurity Education National Protection and Programs Directorate
Vu Nguyen	IT Specialist U.S. Customs and Border Protection
Bill Noonan	Assistant Special Agent in Charge, Criminal Investigative Division U.S. Secret Service
Keri Nusbaum	Director of Recruitment and Development National Protection and Programs Directorate
Bill Pachucki	Director of the Cyber Threat and Assessment Center Office of the Chief Information Officer
Ian Quinn	Deputy Assistant Director of the Cyber Crimes Center U.S. Immigration and Customs Enforcement
Ben Scribner	Program Analyst National Protection and Programs Directorate
Temea Simmons-Collins	Chief of the Promotions Assessment Branch U.S. Customs and Border Protection

Robert Simpson	Chief of the Entry-Level Assessment Branch U.S. Customs and Border Protection
Chad Sonnenfeld	Information Security Office of the Chief Information Officer
Roberta Stempfley	Deputy Assistant Secretary, Office of Cybersecurity & Communications National Protection and Programs Directorate
Jaime Vargas	Chief Information Security Officer Office of the Inspector General
Jill Vaughan	Chief Information Security Officer Transportation Security Administration
Mark Weatherford	Deputy Undersecretary for Cybersecurity National Protection and Programs Directorate
Robin Williams	Director of the National Cybersecurity Education & Workforce Development Office National Protection and Programs Directorate
Brian Zeitz	Chief, Incident Management, US-CERT National Protection and Programs Directorate