



## Cyber-related Government Jobs

[Kathryn Stephens, NSCI](#)

August 2, 2010

### U.S. Cyber Command



U.S. Cyber Command was established to plan, coordinate, integrate, and conduct cyberspace activities throughout the Department of Defense. Additionally, all of the military branches have organizations that report to Cyber Command and are dedicated to cyberspace security. The Air Force activated the 24<sup>th</sup> Air Force in April 2009, and the Marines established the Marine Corps Forces Cyberspace Command at Fort Meade in January 2010. The Navy launched the U.S. Fleet Cyber Command in February 2010, and the Army Forces Cyber Command will be fully operational in October 2010.<sup>1</sup> The Pentagon has reported that there will be around 1,000 cyber security positions in Fort Meade for the new Cyber Command, and Maryland Gov. Martin O'Malley (D) said that the total command will exceed 21,000 soldiers and civilians.<sup>2</sup> Current job opportunities: <http://usajobs.gov/>.

### National Security Agency



The National Security Agency (NSA) works to enable "Network Warfare operations to gain a decisive information advantage for the Nation." NSA cybersecurity professionals aim to dominate global cryptology; secure national security systems; and connect people, systems and information on a global scale.<sup>3</sup> The NSA also hosts the Cyber Defense Exercise (CDX) annually, which allows cybersecurity professionals to compete to prove their skills in network defense and incident response. CDX provides an opportunity for cybersecurity students to find NSA and other government agency jobs. Employment opportunities: [http://www.nsa.gov/careers/opportunities\\_4\\_u/index.shtml](http://www.nsa.gov/careers/opportunities_4_u/index.shtml).

### Department of Defense Cyber Crime Center



The U.S. Department of Defense (DoD) is looking for cybersecurity workers for the DoD Cyber Crime Center (DC3). The DC3 assists in criminal, counterintelligence, counterterrorism and fraud investigations and also provides computer investigation training to DoD members who work on DoD information systems. Employment opportunities: <http://www.dc3.mil/dc3/dc3Jobs.php>.

### U.S. Air Force



The U.S. Air Force (USAF) has turned to civilian federal employees and contractors to fill cybersecurity positions. The USAF has been authorized to use the streamlined Schedule A hiring authority, which allows workers to bypass the normal competitive process. The USAF is looking to fill positions in incident handling; malware/vulnerability analysis; cyber risk and strategic analysis; cyber vulnerability detection and assessment; intelligence analysis; cyber incident response and network and system engineering.<sup>4</sup> Employment opportunities: <http://www.afciviliancareers.com/index.php>.

<sup>1</sup> <http://fcw.com/articles/2010/07/26/feat-cyber-command-launch-timeline.aspx>

<sup>2</sup> [http://www.gazette.net/stories/05282010/businew174314\\_32560.php](http://www.gazette.net/stories/05282010/businew174314_32560.php)

<sup>3</sup> [http://www.nsa.gov/about/strategic\\_plan/index.shtml](http://www.nsa.gov/about/strategic_plan/index.shtml)

<sup>4</sup> <http://www.thenewnewinternet.com/2010/07/16/air-force-expands-hiring-authority-for-cyber-jobs/>



## Cyber-related Government Jobs

[Kathryn Stephens, NSCI](#)

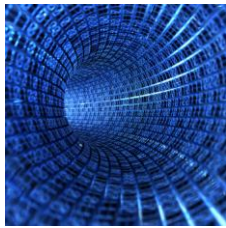
August 2, 2010

### U.S. Navy



Navy Chief Information Officer Rob Carey released the Navy Cyber/IT Workforce Strategic Plan for fiscal 2010 through 2013 on July 16. The plan focuses on integrating technology into business processes and recruiting IT professionals that also have business skills. The plan also focuses on telecommuting to attract and retain IT professionals. Carey says that information technology is vital to naval operations, and “every IT professional in the Navy and Marine Corps has to think of themselves as a warrior.”<sup>5</sup> Employment opportunities: <http://www.public.navy.mil/usff/cyberfor/Pages/default.aspx>.

### Department of Commerce



The Department of Commerce (DoC) is working to protect consumers from sophisticated cyber threats, and is also looking at new ways to use the Internet to foster economic growth and innovation. The DoC is addressing cyber concerns through the National Institute of Standards and Technology, the National Telecommunications and Information Administration, and their Internet Policy Task Force. The Task Force will work on public policy and operational challenges on the Internet to ensure that the Internet remains open for innovation. DoC employment: <http://www.commerce.gov/about-commerce/careers>.

### Department of Homeland Security



In October of 2009 the Department of Homeland Security (DHS) announced that it would hire up to 1,000 cybersecurity professionals over the next three years.<sup>6</sup> DHS is specifically looking for workers for cyber incident response, cyber risk and strategic analysis, vulnerability detection and assessment, networks and system engineering, and intelligence and investigation. Employment opportunities: [http://www.dhs.gov/xabout/careers/gc\\_1240512546017.shtm](http://www.dhs.gov/xabout/careers/gc_1240512546017.shtm).

### Federal Bureau of Investigation



The FBI is the lead law enforcement agency responsible for investigating cyber cases including cyber-based attacks and high technology crimes. The FBI has a devoted Cyber Division which coordinates the agency's efforts to combat cyber threats and also supports other FBI priorities including counterterrorism, counterintelligence and other criminal investigations. There are career opportunities with the FBI's Cyber Division in computer intrusions, computer crimes, special technologies and applications, and information sharing and analysis. Students with knowledge in digital forensics and investigation may be well suited for a career with the FBI Cyber Division. Employment opportunities: <http://www.fbijobs.gov/311132.asp>.

<sup>5</sup> [http://www.nextgov.com/nextgov/ng\\_20100719\\_1797.php](http://www.nextgov.com/nextgov/ng_20100719_1797.php)

<sup>6</sup> [http://www.govinfosecurity.com/articles.php?art\\_id=2037&pg=4](http://www.govinfosecurity.com/articles.php?art_id=2037&pg=4)