People and processes outweigh technology in effective government information security

by Courtney Jewell

U.S. Government Security Mandates Heighten Workforce Professionalism and Preparedness, Analyst Study Finds

The International Information Systems Security Certification Consortium, the non- profit global leader in educating and certifying information security professionals throughout their careers, today announced the U.S. government- specific results of the third annual Global Information Security Workforce Study, conducted by global analyst firm IDC and sponsored by (ISC)2. According to the report, the U.S. government's efforts to improve its overall security posture through compliance with stringent information security mandates is increasing the professionalism and preparedness of its information security workforce.

The 2006 Global Information Security Workforce Study was conducted by IDC to provide detailed insight into the important trends and opportunities within the information security profession. For the second year, study authors broke out a separate government-specific report to gain a clearer understanding of the specific issues challenging the public sector, how the information security profession is being impacted by those challenges, how information security professionals are compensated compared to other sectors and what steps are needed to advance their careers and the profession.

The study found that public sector compliance mandates such as the Federal Information Security Management Act (FISMA) and Department of Defense Directive 8570.1, as well as concern over the large number of recent high- profile security breaches and the rise in cyber terrorism, are driving agencies to invest nearly half of their total information security budgets on personnel specialized training and certifications. "This report clearly illustrates the U.S. Government's understanding that its information security cannot be achieved solely through the use of technology solutions; any strategy that is going to effectively protect and secure information assets and networks must be underpinned by a well-trained, educated, professionalized workforce," stated Lynn McNulty, CISSP, director of government affairs for (ISC)2.

The study found that federal, state and local governments now spend, on average, 46 percent of their total security budgets on personnel and training- with increasing demand in the top three areas of C&A, information risk management and forensics. This statistic moves the government towards being on par with the private sector, which spends 49 percent of its security budgets on hiring and training, the study says.

Compliance requirements are also raising hiring and career advancement standards for the information security profession. IDC reported that over 95 percent of defense sector respondents and over 92 percent of non-defense sector respondents believe that it is somewhat or very important for job candidates to hold professional certifications. Almost 70 percent of defense- sector respondents said that their stance on the issue

was largely because of the DoD Directive 8570.1, which requires all information security personnel who have access to DoD privileged systems to obtain professional certifications accredited by ANSI under the ANSI/ISO/IEC 17024 standard over the next three years.

The report forecasts that the growing demand for qualified information security professionals by federal, state and local governments will remain a priority for the foreseeable future, with governments seeking individuals not only with technical skills but also softer business skills in areas like collaboration, communication and negotiation to help drive management buy-in and successful execution of agency policies.

IDC used a Web-based electronic survey to collect and analyze the responses of 373 information security professionals from U.S. federal, state and local agencies and government contractors. Other highlights from the 2006 government-specific report include:

* C&A training was the most sought-after type of information security training across the federal government in 2006. Among survey respondents, C&A remained the top interest for defense sector information security professionals and for the first time this year came out ahead of business continuity and disaster recovery among non-defense sector workers.

* Information security personnel within the federal government, on average, have more experience and make equal or greater salaries than their private sector counterparts, though non-defense federal workers earn more than their counterparts in the defense sector and state and local governments. Non-defense sector information security professionals earn an average salary of $107,957, compared to $98,052 for defense workers and $79,709 for state and local workers.

* The role of the Chief Information Security Officer (CISO) is progressing in status, thanks to changing reporting structures driven by compliance with security mandates and increased attention to security breaches. Among federal respondents, CISOs have passed CEO-equivalent managers to reach the No. 2 spot just below CIOs as the role most responsible for agencies' information security functions. Over time, IDC predicts that CISOs will be better positioned to drive government-wide awareness and promote interagency cooperation on information security efforts.

* Technologies of interest to federal, state and local governments include biometrics, wireless security and forensic tools. IDC predicts that over the next 12 to 24 months, federal, state and local governments will focus more on risk management and forensics in response to recent data breaches from malicious hackers and employee negligence.

The report concluded that the market outlook for information security professionals seeking employment in the federal government is strong. Opportunities are especially abundant for information security professionals who recognize that certification is increasingly important to not only hiring but career advancement within the

federal government; that opportunities for specialization exist in the areas of C&A, audit and forensics; and that information security professionals in the public sector will spend much of their time dealing with meeting regulatory compliance requirements, achieving C&A of information systems and researching new technologies.

To download a copy of the study, please visit http://www.isc2.org/workforcestudy.

People and processes outweigh technology in effective government information security by Courtney Jewell