Postal Service to credential users of federal websites

By ANDY MEDICI
amedici@federaltimes.com

PHOTO ILLUSTRATION BY JOHN BRETSCHNEIDER/STAFF

If the Federal Cloud Credential Exchange program is successful, visitors will be able to use existing credentials from private companies to log into federal websites.

The U.S. Postal Service is planning to partner with the private sector to create a more secure way for taxpayers to log on to federal websites to conduct business or seek government services.

The digital Federal Cloud Credential Exchange platform will launch in early 2014 as a pilot project to gauge agency and industry interest and plot a revenue model, according to USPS spokeswoman Darleen Reid-Dameo.

Here is how it will work:

■ Private companies with highly secure login procedures — such as banks — would sign up to be identity providers for the system. Agencies would sign on to participate as well.

■ Individuals would sign in to agency websites and services by using their own login provided by the private company instead of having to create multiple usernames and passwords.

■ The Postal Service would connect the systems and manage the overall program.

The Veterans Affairs Department and the General Services Administration have already signed on to participate, according to the Postal Service.

The potential for savings is considerable, according to Andre Boysen, the chief marketing officer for SecureKey Technologies Inc., the contractor developing the system. This model would enable federal agencies to forgo verifying identities themselves, offer services faster and reduce fraud.

In 2012, SecureKey launched a similar platform that allows Canadians to use their banking logins to access government services, including health benefits and student loan information.

"You get better business services with a lower cost and a happier customer," Boysen said.

He said private companies such as banks have a better idea of how their customers behave and can better recognize fraudulent users and activities. This creates a higher level of security when those users try to access federal programs.

"Agencies are already on the hook for fraud, and this system can help reduce that," Boysen said.

He added that people often must remember numerous usernames and passwords for their everyday lives, and remembering one for each agency they work with can be burdensome. Having a login they use every day will prevent agency customers from forgetting or misplacing login credentials.

Experts agree that agency efforts to create more secure login credentials will grow.

Steve O'Keeffe, founder of public-private IT partnership MeriTalk, said federal efforts to create more secure credentialing systems will increase as agencies move more services to the cloud.

He said earlier efforts to allow agency clients to use the Internet to apply for services and work with agencies created two tiers of agency services — one paper and one online — that did little to reduce inefficiency and waste in service offerings.

"This effort is going to become more and more important as time goes on," O'Keeffe said,

Pam Walker, a senior director at TechAmerica, said identity management and credentialing services are an important and growing field in the public sector. She said all companies and agencies have to figure out how to address who has access to what kind of information and how to best manage customer identity.

"There is a lot of money in streamlining the system and making it more secure — such as reducing fraud in the government benefits area," Walker said. ☐

NSA director: Furloughs have damaged us

By NICOLE BLAKE JOHNSON
njohnson@federaltimes.com

While many employees in the intelligence community are back on the job after being furloughed earlier this month, the government shutdown has taken a toll on workplace morale.

"The furloughs hurt morale, even though we've brought everybody back," Army Gen. Keith Alexander said at a telecommunications event last week. "When you look at the numbers of Ph.D.s, mathematicians and computer scientists we have both at Cyber Command and NSA [National Security Agency] and the way we are treating them with this furlough, it's flat wrong. We should be better."

At NSA, there are 4,000 computer scientists, 1,000 mathematicians and more than 900 Ph.D.s, Alexander said. His concern is the lasting and damaging impact the shutdown will have on the morale and recruiting of people with such specialized skill sets.

"We're making it hard for them to stay in the government," Alexander said of younger employees, while speaking at a separate cybersecurity event last week. "How do you get good talent to come to the government when we treat them like that?"

On day two of the shutdown, Director of National Intelligence James Clapper told a Senate panel that intelligence agencies were forced to furlough about 70 percent of their civilian employees.

Since then, NSA, the Defense Department, the CIA and others have called employees back.

CIA Director John Brennan last week recalled employees who perform core missions, such as foreign intelligence collection, all-source analysis, covert action and counterintelligence.

"I have made this decision because of the potential adverse cumulative and unseen impact on our national security from the now week-long furloughing of a significant portion of the CIA workforce, as keeping our staffing at the dramatically reduced levels of the past week would pose a threat to the safety of human life and the protection of property," Brennan said in an Oct. 8 statement.

CIA spokesman Dean Boyd declined to say how many employees were being brought back or how many had been furloughed.

In fiscal 2012, the CIA had about 22,200 employees, said Steven Aftergood, a government secrecy expert at the Federation of American Scientists, citing classified information released by former government contractor Edward Snowden.

Others agree that the furloughs and government shutdown will harm morale and turn away talent.

"I find it hard to believe that this wouldn't have an impact, shift perceptions and impact [the] talent pool," said Tara Maller, a research fellow at the public policy group New America Foundation.

Speaking at the same cyber event as Alexander, Maller said it is hard enough for agencies to devote the resources and pay competitive salaries for top talent.

For people contemplating leaving NSA, the current environment makes their decision easier, said Trey Hodgkins, senior vice president of the global public sector at the trade association TechAmerica. Agencies have to understand their workforce needs, respect their employees and pay them appropriately. ☐

Sean Reilly contributed to this report.

Report: Iranian hackers breached U.S. Navy intranet

Sailors are continuing to encounter intranet delays as security updates are installed — updates that may or may not be tied to an alleged hacking by Iran.

Iranian agents or proxies breached the Navy's unclassified computer network sometime during the past few weeks, according to a Sept. 27 report by the Wall Street Journal.

The cyber-trespassers did not steal any secrets, but their presence alarmed the Pentagon.

The Defense Department declined to confirm the report of a breach, saying only that DoD networks see "daily attempts" by hackers and that these defenses are updated constantly to parry them.

"As a matter of policy and for reasons of operations security, we do not comment on the details of our operations to counter cyber threats or any allegations made in recent media reports," DoD spokesman Lt. Col. Damien Pickart said in a statement. "We have full confidence in the integrity of the department's networks and systems upon which we conduct critical operations. This recent reporting does not change that assessment."

Wide swathes of the Navy's websites have been down or intermittent in recent days because of security upgrades.

Navy officials said in a Sept. 20 news release that networkwide outages related to the updates could last "over the coming weeks."

A spokesman with Fleet Cyber Command would not say when the upgrades would end nor offer specific systems that would go offline, citing security concerns.

When asked whether the upgrades were related to alleged hacking, the spokesman said, "We do not discuss the details of network operations for security reasons."

The Navy-Marine Corps Intranet has an estimated 800,000 users.

Navy Personnel Command has posted a guide on its website for getting personnel records information during the outage at www.public.navy.mil/bupers-npc. ☐

From staff reports