nextgov TECHNOLOGY AND THE BUSINESS OF GOVERNMENT

SEARCH

NEWS BLOGS CHANNELS THE BASICS EVENTS

SUBSCRIBE TO eNEWSLETTERS & ALERTS

EMAIL

PRINT

SHARE

NEWSWIRE

Illinois man denies taking military data to China
04/15/2011

White House draft bill expands DHS cyber responsibilities
04/15/2011

USAID works around FISMA to use iPads
04/15/2011

Soldiers' Wearable Computers May Get an iPhone Brain
04/15/2011

MORE NEWS...

RESOURCES

Tech Channels

Top Technology Contractors

Managing Technology Archive

Quiz: How Much 2.0 Do You Know?

The Feed: What Feds Are Twittering

Word-By-Word: Federal Tweets

What Transparency Means to Feds

Making Great Gov Web Sites

Cyber identity strategy would eliminate the need for multiple passwords

BY ALIYA STERNSTEIN 04/15/2011

The White House on Friday unveiled guiding principles for industry on developing identity credentials that would allow ID holders to log on to virtually any website, eliminating the need to remember multiple passwords or to enter personal information.

The 52-page National Strategy for Trusted Identities in Cyberspace, first suggested in a 2009 cyberspace policy review ordered by President Obama, represents the start of a public-private partnership to ease online commerce while protecting privacy. Globally, companies conduct $10 trillion worth of business online, according to federal estimates. The Obama administration opted to house the effort at the Commerce Department, inside an office that acts as a liaison between the federal government and industry.

Federal officials have stressed the ID technology is voluntary. On Friday, Commerce Secretary Gary Locke dismissed rumors that it would be a national ID card or driver's license for the Internet that would enable the government to track citizens' every move online. The strategy calls for adopting standards that limit the kinds of information services can collect. Those standards would stipulates how such data is to be used.

"I'm optimistic that NSTIC will jump-start a range of private sector initiatives to enhance the security of online transactions," Locke said at a launch event the U.S. Chamber of Commerce hosted. "This strategy will leverage the power and imagination of entrepreneurs in the private sector to find uniquely American solutions."

The administration acknowledges the concept -- referred to as an identity ecosystem -- will take many years to implement and require buy-in from international and private sector partners.

Going forward, the role of the federal government in the initiative will be to protect individuals, support industry through workshops and research funding; work with the private sector to ensure the tools are compatible; provide and accept government services using credentials, and lead by example in deploying credential systems internally.

The National Institutes of Health, in coordination with patient advocates and pharmaceutical firms, already has adopted an identity technology to speed the enrollment of patients in clinical trials, including a cancer therapy evaluation program. In the past, paper signatures were required for every stage of the clinical trial approval process, delaying treatment. And passwords were not an option. "Passwords just won't cut it here as they are too insecure and the stakes are too high to risk fraud," Locke said.

The technologies should prevent online services from monitoring people's credential use so companies cannot follow their customers' activities online, according to the strategy. The tools would be programmed in such a way that they can be remotely suspended if they fall into the wrong hands. Organizations would have to accept multiple credential formats, similar to how ATM machines accept cards from different banks.

Research shows that, partly because passwords are insecure, 8.1 million American adults were hit by identity theft or fraud last year. For example, hackers employ a practice known as phishing to lure victims into entering

MOST READ | MOST EMAILED

Budget deal threatens government cloud security clearances

U.S. law enforcement agencies struggle to detect cyberattack sponsors

IT reforms save taxpayers $3 billion in less than five months, fed CIO says

LATEST BLOG POSTS

WHAT'S BREWIN'
The Next Big Tsunami?
BY BOB BREWIN 04/15/11 03:47 pm ET

WIRED WORKPLACE
Number of IT Grads Increases
BY BRITTANY BALLENSTEDT 04/15/11 02:43 pm ET

TECH INSIDER
Obama Dishes on Federal Technology
BY KATHERINE MCINTIRE PETERS 04/15/11 01:42 pm ET

CYBERSECURITY REPORT
The FBI Fights Malware with More Lethal Malware
BY ALIYA STERNSTEIN 04/15/11 11:45 am ET

HEALTH IT UPDATE
"Meaningful Use" Timelines Slip
BY JOHN PULLEY 04/15/11 05:03 pm ET

BLOGS HOMEPAGE

passwords, Social Security numbers, bank accounts or other details that can be used to discern passwords on to fake sites that harvest their identities.

Jane Holl Lute, deputy secretary of the Homeland Security Department, who also attended Friday's event, said the aim of NSTIC is not to regulate Internet transactions, but rather engender honesty in online exchanges.

"In cyberspace, can we still trust each other?" she posited. "The goal here is confidence, not centralized control."

The strategy sets out several milestones. For instance, within five years, the program office should develop metrics to measure the progress of the effort, including broad participation, compatibility, choice of a variety of credentials, acceptance at federal agencies, and "trust marks" -- emblems that indicate an organization has complied with the ecosystem's rules. After a decade, the benefits of the ecosystem are supposed to be available to every individual; all policies and technologies are to be in place; a majority of online organizations should be part of the enterprise and a sustainable market for credential providers should emerge.

If the idea of NSTIC is embraced, a person could access secure websites with one so-called trusted identity, which could be stored on, for example, a smart card, key fob or piece of software embedded in a smart phone.

Commerce officials provided the example of a woman who downloads a digital certificate from an ID provider onto her cellphone. She keys in a short password to prove her identity and is then able to conduct from the phone all her online transactions, including paying her taxes. Through such single sign-on mechanisms, a doctor could insert a smart card into his computer to access a federal website after an earthquake and see where medical attention is needed. The site might show that a nearby triage center requires help from a specialist with his background. When he arrives at the center, he could swipe the card to quickly confirm that he is a specialist and start treating victims.

The strategy was applauded by many in industry who say the administration listened to their advice in crafting the policy.

"If it comes to the point where I can validate and ensure my identity online, and they don't need to know anything except that I have a trusted identity, I don't have to give up any other information; I don't have to give up my mother's maiden name," explained on Jennifer Kerber, a vice president of the trade group TechAmerica.

Some privacy groups said they are pleased with the approach the federal government has taken, but the outcome largely depends on the will of industry to follow the rules.

Leslie Harris, president of the Center for Democracy and Technology, a privacy group, said she views the technology as the opposite of a national ID card, because it would hide the individual's personal information. In fact, the current habit of using the same password on multiple sites is just as dangerous as a national ID card because perpetrators who crack a password can then monitor a person's online behavior.

"Now the question is whether industry can step up and enforce a serious governance model in a way that's protective of privacy," she said.

But other civil liberties organizations are more skeptical.

"A top-down strategy for online identity is unlikely to work," said Jim Harper, director of information policy studies at the libertarian Cato Institute. "Trust is not created by government-corporate consensus, but by the hot forge of the marketplace. People will not participate in a government-corporate identity project that deviates from their demand for control of identity information, which is an essential part of privacy protection, autonomy and liberty."

He dismissed the notion that the technology is akin to an online driver's license, however. "People who talk about an Internet driver's license don't know enough about identity systems, the Internet or metaphors," Harper said.

Stay up-to-date with federal technology news alerts and analysis - sign up for Nextgov's email newsletters.

By using this service you agree not to post material that is obscene, harassing, defamatory, or otherwise objectionable. Although Nextgov does not monitor comments posted to this site (and has no obligation to), it reserves the right to delete, edit, or move any material that it deems to be in violation of this rule.

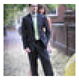
SHOWING 0 COMMENTS

Sort by Newest first ▾ Subscribe by email Subscribe by RSS

ADD NEW COMMENT

Optional: Login below.

REACTIONS



E5V 04/15/2011 06:37 PM

From Twitter One more retweet from lmoliva_

RT @timhartman: RT @Nextgov Cyber identity strategy would eliminate the need for multiple passwords http://tinyurl.com/3qh4r9s

timhartman 04/15/2011 05:23 PM

From Twitter

RT @Nextgov Cyber identity strategy would eliminate the need for multiple passwords http://tinyurl.com/3qh4r9s

vera_newhouse 04/15/2011 02:33 PM

From Twitter

RT @NextGov: Cyber identity strategy would eliminate the need for multiple passwords http://tinyurl.com/3qh4r9s

NextGov 04/15/2011 02:03 PM

From Twitter

Cyber identity strategy would eliminate the need for multiple passwords http://tinyurl.com/3qh4r9s

GetPregnant_ 04/15/2011 12:52 PM

From Twitter

Cyber identity strategy would eliminate the need ... - Nextgov: Commerce officials provided the example of a wom... http://bit.ly/gNCm4d

comments powered by **DISQUS**

ABOUT US MEDIA KIT FAQ PRIVACY POLICY NEWS FEEDS SITE MAP