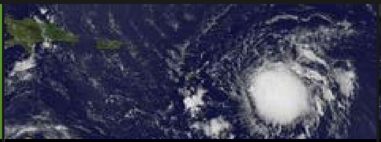
Share 53
Tweet 89
Share 9
Share 170

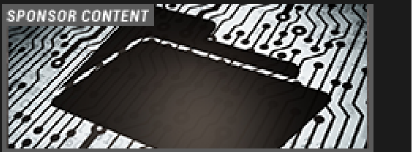
Print this article
Email this article
Increase size

ET // IRS BREACH // CYBERWARRIORS // SOCIAL MEDIA



Secure Your Spot for Sept. 9th!
NOAA Sends Drone Right into Erika

'Disrupting' Government Is Hard Work

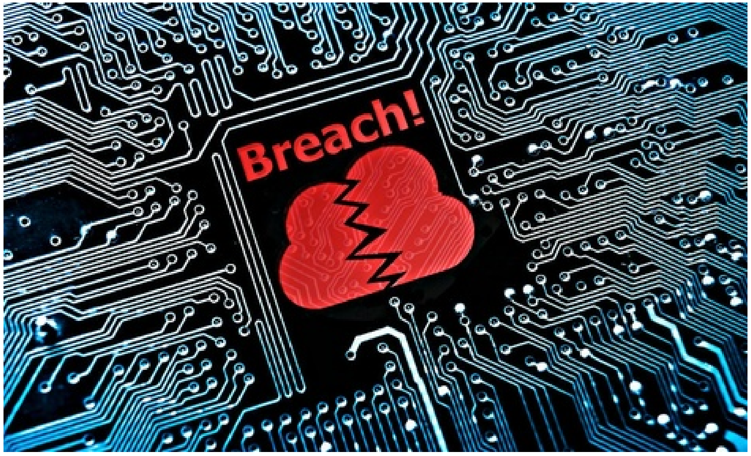


SPONSOR CONTENT
Expert Q&A: Protecting Digital Content

NEWS CIO BRIEFING EMERGING TECH CLOUD CYBERSECURITY MOBILE HEALTH DEFENSE BIG DATA

SEARCH NEXTGOV SEARCH

PENTAGON UNVEILS NEW RULES REQUIRING CONTRACTORS TO DISCLOSE DATA BREACHES



wk1003mike/Shutterstock.com

By Aliya Sternstein
August 26, 2015
4 Comments

NEXTGOV NEWSLETTE
SUBSCRIBE

RELATED STORIES

With a Major Cybersecurity Job Shortage, We Must Act Like We Are at War
11 Comments

Is the Ashley Madison Hack Real a National Security Risk?

Feds Expect to Spend at Least $500 Million on the Next Five Years of Data Breaches
1 Comment

Pentagon Contractors Rank Below Retailers and Banks When it Comes to Cybersecurity
5 Comments

New sweeping defense **contractor rules** on hack notifications take effect today, adding to a flurry of Pentagon IT security policies issued in recent years.

Just this month, the Office of Management and Budget **proposed guidelines** to homogenize the way vendors secure data governmentwide. The Defense Department had already released three other policies that dictate how military vendors are supposed to handle sensitive IT.

Now, industry, which is already concerned about overlapping and burdensome cyber rules, worries the Pentagon will go back and retroactively change contracts, after the White House draft is finalized.

The new Pentagon regulations for "Network Penetration Reporting and Contracting for Cloud Services" cover more types of incidents and more kinds of information than past policies. The guidelines, which were published Wednesday, also apply to a broader

MORE FROM NEXTGOV CLOSE [X]
18F Awards 16 Firms Spots on Agile BPA
Leave a comment

swath of the contracting community.

The objective here is to more tightly control the way defense data traverses contractor systems and is stored by companies, military officials say.

"The benefits of the increased security requirements implemented through this rule are that more information will be protected from release, inadvertently or through malicious intent," and in so doing strengthen national security," Jennifer Hawes, editor of the Defense Acquisition Regulations System, said in the policy.

Ongoing attacks against military contractors prompted the release of Wednesday's regulations, according to the Pentagon.

The "interim rule" will kick in before a public comment period because of "the urgent need to protect covered defense information and gain awareness of the full scope of cyberincidents being committed against defense contractors," Hawes said.

It is unclear whether this is a specific hacker campaign -- or the usual targeting of high-value contractors. *Nextgov* has asked the Pentagon to elaborate. Parts of the rule were originally required by Congress in the 2013 and 2015 National Defense Authorization Acts.

The policy applies to contractors, subcontractors and lower-tier, downstream vendors. There also is a provision for cloud computing services that spells out standard contract language for purchases.

The measure covers confidential military technological and scientific data, known as “unclassified controlled technical information," as well as all other unclassified "protected" data, such as export-controlled information. The protection of classified information is governed by other measures.

Within 72 hours of detecting an incident or possible incident, subcontractors and contractors must notify Defense through this **website**.

The Pentagon, in turn, will be required to protect the confidentiality of proprietary and identifying information that contractors submit to the government for investigation.

"Recent high-profile breaches of federal information show the need to ensure that information security protections are clearly, effectively and consistently addressed in contracts," Hawes said.

Over the past year, the U.S. government has confirmed hacks that exposed sensitive data at the Office of Personnel Management, State Department, White House and U.S. Postal Service.

In the rulemaking, Hawes said this latest "rule does not duplicate, overlap or conflict with any other federal rules."

‘I Fear Confusion’

But the contracting industry contends the Pentagon and OMB are out of lockstep in moving forward with data security guidelines. The public can comment on the OMB draft guidelines until Sept. 10.

“It seemed a little ironic that you're putting into place a more detailed, specific, focused DOD rule” while guidance for the whole federal government is open for a 30-day discussion period, before even getting down to the nitty gritty of contract clauses, said Alan Chvotkin, executive vice president of the Professional Services Council, an

Read more

BLOGS

DISA Issues Pentagon-Friendly Cloud Computing Guide
Emerging Tech by Frank Konkel

Here’s Why ‘Disrupting’ Government Is Such Hard Work
Tech Insider by Winston Chang

Why NASA’s 20-Year-Old Astronaut Hiring Process Still Works Today
Wired Workplace by Nate Regier

industry group.

It could be years before the government incorporates the White House guidelines into the official federal acquisition rules, and then decides whether to fold those rules into existing defense contracts, he said.

“Companies hate any time when you retroactively are substantially changing the terms and conditions of a contract,” Chvotkin said.

The public has two months to comment before the Defense regulatory document is finalized.

There may be additional cyber contract conflicts in the offing, Chvotkin said.

On June 18, the National Institute of Standards and Technology issued guidelines for potential contractor clauses involving the protection of sensitive “controlled unclassified” information inside company systems. The Pentagon in May 2014 released rules specific to defense contractors on counterfeit electronic parts, which aim to address the problem of suppliers damaging computerized military systems. That follows a separate set of November 2013 contractor stipulations for guarding unclassified controlled technical information.

“We've been supportive of taking a governmentwide look at standardizing reporting requirements, whatever they happen to be, 72 hours, fantastic; if it’s 48 hours, if it’s 24 hours. There ought to be some minimum governmentwide statutory provisions,” Chvotkin said, citing various potential breach notification deadlines. With the defense rule, "I fear confusion rather than clarity.”

10,000 Contractors Affected

By contrast, Pentagon officials describe their measure as an umbrella policy.

The regulation "expands on the existing information safeguarding policies" in the defense contractor compendium of rules, and it "requires contractors to report cyberincidents to the government in a broader scope of circumstances," Hawes said.

Specifically, companies must report all events that result in "an actual or potentially adverse effect" on a secure information system or data inside that system. They also must inform Defense about cyberincidents that impair a contractor’s ability to provide the military critical support.

Military contractors will have to let department personnel inside company facilities to perform a forensics analysis of equipment and information potentially impacted by the incident.

Some 10,000 companies are covered by the rule, with small businesses comprising under half that number.

Defense says the regulation should rein in redundant reporting processes and create a single contact point. The regulation would create a "single reporting mechanism" for informing Defense of such events, Hawes said.

Companies must submit any malware found, as well as preserve images of all affected systems and relevant monitoring data for at least 90 days, in case the government needs to investigate further.

Officials say the steps contractors must follow under the new policy will reduce their security tasks by 30 percent.

Defense contractors are constantly under attack by cyberspies, and in some cases, by their own careless employees.

Federal officials have said they cannot be positive about the extent of breaches of government employee data held by background investigators USIS and KeyPoint Government Solutions, because neither had sufficient logs. China is believed to have raided personnel files to glean intelligence on U.S. national security operations.

Separately, a Senate Armed Services Committee **report** released last fall claims Chinese-sponsored hackers pierced the networks of U.S. Transportation Command contractors at least 20 times from June 2012 through June 2013.

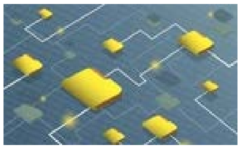
Suspected Chinese attackers compromised trade secrets at ID security company RSA in 2011, and then used the stolen data to crack open the locks on Lockheed Martin's RSA-protected network. Lockheed quickly subdued the intruders, in that instance.

(*Image via* ***wk1003mike****/ Shutterstock.com*)

RECOMMENDED FOR YOU

- **Video: The Closest You Can Get to Space Without Leaving Earth**
- **Why More Agencies Tap Twitter to Recruit New Talent**
- **US Military Is Replacing the Humvee with a Huge Truck that Looks Like an Angry Shark**

ADD A COMMENT



Developing Strategies to Protect Digital Content

Enable Workforce Collaboration

Last Chance to Register!

Sign Up for Government Rewritten

JOIN THE DISCUSSION

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.

Nextgov

About // Contact Us // Events // Advertise // List Rentals // Site Map // Privacy Policy // Terms & Conditions

GovExec // Defense One // Quartz // National Journal // The Atlantic // CityLab