



IG: DHS Struggles with Cyber



OPEM Security Overhaul Under Scrutiny



CIOs: Share Legacy IT Horror Stories



Is Your Incident Response Plan Ready?

PENTAGON UNVEILS NEW RULES REQUIRING CONTRACTORS TO DISCLOSE DATA BREACHES



wk1003mike/Shutterstock.com

By [Aliya Sternstein](#)

August 26, 2015

[4 Comments](#)

**NEXTGOV
NEWSLETTER**
[SUBSCRIBE](#)

RELATED STORIES

**Federal Inspectors
Want to Double-
Check How Agencies
Fared During 'Cyber
Sprint'**

**Contractors Say
Proposed Hack
Reporting Rules
Aren't Strict Enough**

**Intelligence Chief:
OPM Hack Was Not a
'Cyberattack'**

[12 Comments](#)

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

[5 Comments](#)

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

199 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 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.

[Print this article](#)
[Email this article](#)
[Increase size](#)

SEARCH NEXTGOV

SEARCH

Sapient Government Services

DIGITAL TRANSFORMATION FOR THE PUBLIC SECTOR

[SEE WHAT BOLD THINKING CAN DO >](#)

PROMOTIONS



INSIGHT REPORT **Raise Your
Agency's Energy I.Q. with Smart
Technologies** // [Read more](#)



ISSUE BRIEF **Arkansas Shows the
Nation the Value of Health Data
Analytics** // [Learn more](#)



REPORT **Fighting Fraud in State &
Local Government** // [Read more](#)



REPORT **Using Big Data to Drive
Public Sector Insights** // [Learn more](#)

FREE NEWSLETTERS

☐ Nextgov Today

☐ Health IT

☐ Route Fifty Today

☐ Research & Insights

☐ Nextgov ThreatWatch

[SEE ALL](#)

Enter your email address here...

SUBSCRIBE

**OUR SYSTEMS
DON'T SUPPORT
ORGANIZATIONS.
THEY DRIVE THEM.**

[LEARN MORE](#)

LOCKHEED MARTIN

BLOGS



**Federal Agencies: What's Your Hack-
Response Plan?**

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 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



Emerging Tech by Frank Konkel

Time Has Come to Reform Laws Governing Law Enforcement Access to Data

Tech Insider by Paul Rosenzweig

How Companies Are Using LEGOs to Unlock Talent Employees Didn't Know They Had

Wired Workplace by Jenn Choi

SPONSORED LINKS

Top Vacations8 Must See Vacation Spots. This is where your next vacation needs to be...
[Newszoom](#)

10 Things to Start DoingBecome more successful by doing these 10 things each day.
[Newszoom](#)

Foods that Help Melt FatFatThese 12 foods help to fight weight gain. Are you eating any of them?
[Newszoom](#)

Unbelievable PhotosThese photos are so amazing its hard hard to image they are real!
[Newszoom](#)

Register Now for ACT-IAC's Executive Leadership Conference, Oct. 25-27
Williamsburg Lodge and Conference Center - Williamsburg, VA - Government 2020 - Imagine the Possibilities
www.actiac.org/ELC

Special Offer: Discount Tickets to 2015 Code for America Summit
GovExec readers are eligible for a special discount to the Code for America Summit
<http://www.codeforamerica.org/summit/?discount=RouteFifty-10#register>

Subscribe to Government Rewritten
Get monthly updates on tech trends in mobility, security, and software.
www.govexec.com/govrewritten

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: Upgrading to iOS 9? Here Are Some New Hidden Features

Army CYBERCOM Conducts 'Experiments,' While Navy Cyber Fleet Faces 'Real' Deal

18F's Startup-Friendly Agile BPA Hits First Hurdle -- a Protest

THREATWATCH ALERT [Accidentally leaked credentials / Insider attack](#)

[Contractor Mistakenly Publishes 1.5 Million Confidential Patient I Records on Amazon Web Services](#)

[SEE THREATWATCH REPORT](#)

[ADD A COMMENT](#)



Enable Workforce Collaboration



Sign Up for Government Rewritten



Raise Your Agency's Energy I.Q.



"Innovation in Action Vol. 5" is here!

SPONSORED

Get Smart. Get The D Brief. Subscribe to Defense One's new national security newsletter.

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.

4 Comments

Nextgov

 Login ▾

 Recommend

 Share

Sort by Newest ▾



Join the discussion...

Jamal Tarik • 23 days ago

Yuppies....GREEDY FOOLISH LAZY CON ARTISTS CORPORATE STRATEGY ILLEGALLY BIG DUMB AND FOOLISH TOGETHER TRYING TO OPERATE THE FOOLISH SCAM...

^ | ▾ • Reply • Share ▾

JackChanse • 24 days ago

there are ways to secure data. few thought to spend the money to do it. now there is an incentive: you won't have to report your bad judgment to your big client.

^ | ▾ • Reply • Share ▾

C David Buchanan • 24 days ago

Can we learn something from the OPM with all the SF-86 data in one system? "...homogenize the way vendors secure data government wide" = "...homogenize the way hackers may breach data government wide.

^ | ▾ • Reply • Share ▾

U_S • 24 days ago

Define data breaches. LOL.

^ | ▾ • Reply • Share ▾

 Subscribe

 Add Disqus to your site

 Privacy

[About](#) [Contact Us](#) [Events](#) [Advertise](#) [List Rentals](#) [Site Map](#) [Privacy Policy](#) [Terms & Conditions](#)

[GovExec](#) [Defense One](#) [Quartz](#) [National Journal](#) [The Atlantic](#) [CityLab](#)

© 2015 by National Journal Group, Inc. All rights reserved. | CDN powered by Edgecast Networks