PHIL PIEMONTE, MANAGING EDITOR • E-MAIL: PPIEMONTE@1105MEDIA.COM

OCTOBER 12, 2015 • VOL. 65, NO. 13

FEDERAL EMPLOYEES NEWS DIGEST

Tougher sanctions critical to improving federal cybersecurity

***THIS WEEK, FEND'S NATHAN ABSE INTERVIEWS** Austen Givens, a researcher in cybersecurity at Utica College and former fellow at the Foundation for Defense of Democracies. Givens also has worked at the Department of Defense, Department of Homeland Security, Virginia Fusion Center, and as a staffer for the House of Representatives. His focus has been on cybersecurity in government. Givens has actively studied and commented on the OPM breach of more than 21.5 million federal employees and job applicants, and has emphasized that improved leadership, better training and greater repercussions for careless mistakes could help drive tightened cybersecurity across the federal government.*

What's Inside ▸▸

Some in government have advocated stronger sanctions—even suspending security clearances—for government workers who repeatedly fall for phishing scam emails.

Givens: Yes, they have. I went back to the original article where [Paul Beckman, DHS Chief Information Security Officer] was quoted on this. The spirit of what he is saying is that if you fail multiple ID security audits, then you should have your clearance suspended or revoked. My opinion on this, as I've said, is that if an official repeatedly fails security audits then, absolutely yes, he or she should have their clearance suspended.

What is your reasoning behind that?

Givens: If a senior official at DOD or DHS, for example, were caught bringing home classified documents in their briefcase, then that person would almost certainly be put on administrative leave and investigated and possibly prosecuted. If a senior official were seen leaving a SCIF [Sensitive Compartmented Information Facility] unlocked during the day—and their job was to lock the SCIF—they would definitely be investigated and possibly prosecuted.

So your point is that it is—at least in part—a fairness issue that agencies should be as tough on senior officials as they are on the rest of the staff?

Givens: Yes. There is just zero differ-

PAGE 2 ▸▸

INFORMED INVESTOR

BY EDWARD A. ZURNDORFER

Pre-age 62 FERS annuitants need to understand 'earnings test'—Part II

THIS IS THE SECOND OF TWO COLUMNS discussing how FERS annuitants who retire before age 62 could lose a portion or all of their FERS retiree annuity supplement because of outside earned income. The first column discussed eligibility for and computation of the retiree annuity supplement. This week's column discusses the reduction in the retiree annuity supplement due to excess earned income, which includes salary/wages and net income from self-employment.

A FERS employee who retires before age 62 may lose a portion or all of his or her retiree annuitant supplement if the annuitant is employed and the amount of earned income exceeds the annual exempt amount. Note the following: (1) the reduction applies only to the retiree annuity supplement and not to the FERS annuity; and (2) the reduction for excess earned income does not apply to FERS employees who retire under the special provisions for law enforcement officers, firefighters, air traffic controllers and military reserve technicians until they reach their minimum retirement age (MRA). MRA ranges from age 55 to age 57, and depends upon the year in which a FERS employee was born.

The annual exempt amount is the same as the amount announced and used by the Social Security Administration for the purpose of calculating the reduc-

PAGE 8 ▸▸

PAGE 1

ence between mishandling information in the examples I just gave you—and the ones in your question about failing at general security awareness, including failing to distinguish phishing [and] avoiding clicking on emails that should be perceived as shaky. In both cases, the person is failing one's responsibilities to protect security, whether the document is three-dimensional or virtual. There is no material difference.

You sometimes hear from younger people that this is a younger people/older people issue—the implication being that older, more senior workers don't "get it" about cybersecurity and don't know what they're doing.

Givens: I think that's wrong. But your question does raise a real issue. I think many senior officials do know what they're doing and do it well. But the issue at bottom is that, in practice, there are two sets of rules that apply on IT security in the federal government. One set applies to the worker bees, and the other set applies to Senior Executive Service, GS-14s and the like—the people closer to the top. If I am a lower- or middle-level employee, say at the State Department, and I used my personal email account for official business I'd be in big trouble. And this is not to pick on Hillary Clinton—but because she was Secretary of State, she didn't get the same kind of repercussions she would have had she been a lower-level employee.

Are you saying that a kind of uneven enforcement—the two sets of rules—often applies in practice, and at other agencies too?

Givens: Yes. This happens at other departments too. We've had senior people at DHS clicking on phishing emails, and they are not subject to any kind of heavy repercussions. To me this also illustrates these two separate sets of rules. To me, this is a real organizational—and security—problem.

How do you confront this problem of two sets of rules, and improve the situation?

Givens: This is a key organizational issue. You have to remember these organizations—DHS, DOD, and the rest—have political appointees at the top. And it should be incumbent upon those leaders to emphasize to the rank-and-file that the rules apply to the people at the top as well as to the rank-and-file.

Any other way we could get this across?

Givens: Frankly, the president himself should make it clear to every member of his cabinet that they must take this seriously, and if these senior persons are messing up, then they should be suspended—at least temporarily—until they get this right. The trouble with cybersecurity is that even one little vulnerability can be all it takes. So, if it's a lack of awareness on the part of just one agency head, for example, that permits the Chinese to steal 21-plus million files from OPM, well that's it—they're in! You just have to remember this.

Federal pay back in the news

A LIBERTARIAN THINK TANK has rekindled the debate over federal civilian pay, arguing that federal employees

PAGE 3

OPM trims claims backlog in September

THE OFFICE OF PERSONNEL MANAGEMENT took in 1,000 fewer claims in September than predicted, and processed several hundred more than forecast, helping the agency to score a modest reduction in the number of backlogged claims.

OPM processed 7,944 claims in September, 444 more than the 7,500 claims the agency had forecast. OPM received only 6,300 new claims in the month, exactly 1,000 fewer than it had expected to receive. The new numbers come from OPM's latest claims processing progress report.

The agency ended last month with 14,706 unprocessed claims in its inventory, down from the 16,350 it held at the end of August. That end-of-month total was still higher than the 12,767 backlogged claims it held in its inventory at the end of September 2014. Under its earlier predictions, OPM had hoped to trim its backlog last month to 11,042 claims.

The monthly percentage of claims processed in 60 days or less increased slightly from 69.6 percent in August to 70.1 percent in September. OPM reached a high of 83.7 percent in December. OPM began including the statistic in its monthly progress report in May of last year.

OPM bases its projections on the average number of claims received and processed in the same month each year since 2010.

See the report at: *https://www.opm.gov/about-us/budget-performance/strategic-plans/retirement-processing-status.pdf*.