# IN SUPPORT OF BEN WITTES

Over at Lawfare, Ben Wittes does some brainstorming about what other databases the Chinese may be hacking after ingesting all its OPM winnings. He thinks they might target:

- FDA New Drug Applications
- VA patient records
- Visa applications (State Department)
- Export control applications (Commerce)
- SEC investigative files

For each description of why he thinks they might be juicy targets, he ends with this statement:

> Fortunately, the [XXX] Department is a highly competent counterintelligence agency with first-rate cybersecurity expertise, whose employees are scrupulous about cybersecurity and never do business on their own email servers. I am sure it is fully competent to protect these records.

As it happens, there's plenty of support for most of Wittes' speculative targets, especially if you consult this year's FISMA report from OMB.

**Table 8: CFO Act Agencies' Scores**

| Agency | FY 2014 (%) | FY 2013 (%) | FY 2012 (%) |
|---|---|---|---|
| General Services Administration | 99 | 98 | 99 |
| Department of Justice | 99 | 98 | 94 |
| Department of Homeland Security | 98 | 99 | 99 |
| Nuclear Regulatory Commission | 96 | 98 | 99 |
| Social Security Administration | 96 | 96 | 98 |
| National Aeronautics and Space Administration | 95 | 91 | 92 |
| Department of the Interior | 92 | 79 | 92 |
| Department of Education | 91 | 89 | 79 |
| National Science Foundation | 87 | 88 | 90 |
| United States Agency for International Development (USAID) | 86 | 83 | 66 |
| Environmental Protection Agency | 84 | 77 | 77 |
| Department of Labor | 82 | 76 | 82 |
| Department of Veteran Affair | 80 | 81 | 81 |
| Department of Energy | 78 | 75 | 72 |
| Office of Personnel Management | 74 | 83 | 77 |
| Department of the Treasury | 67 | 76 | 76 |
| Department of Transportation | 63 | 61 | 53 |
| Small Business Administration | 58 | 55 | 57 |
| U.S. Department of Agriculture | 53 | 37 | 34 |
| Department of State | 42 | 51 | 53 |
| Department of Health and Human Services | 35 | 43 | 50 |
| Department of Housing and Urban Development | 19 | 29 | 66 |
| Department of Defense | N/A* | N/A* | N/A* |
| Department of Commerce | N/A† | 87 | 61 |

**Source**: Data provided to DHS via CyberScope from November 15, 2012, to November 14, 2014.
* Due to the size of the Department, the DOD OIG is unable to definitively report a yes or no answer for all FISMA attributes.
† Commerce OIG's FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities. As a result, the FISMA submission primarily focused on assessing policies and procedures, and covered a limited number of systems that would not warrant computation of a compliance score.

Several of the agencies – especially the State Department, but also especially Commerce – rated very poorly in OMB's summary of the Inspector Generals reviews from last year.

I'd add two agencies to Wittes' list: USDA (China has allegedly been stealing seed corn, so why not Ag records?) and Treasury generally (though in some other areas Treasury is pretty good, and it has mostly been "hacked" via old style means – including PII "spillage" – of late).

This list is particularly notable, however, given that the debate over CISA is about to start again. Both Treasury and Commerce are among the agencies that get automatic updates of the data turned over under the law. But their security is, in some ways, even worse than OPM's.

Update: Paul Rosenzweig takes a shot. He picks CFIUS, NRC, FERC, state license DBs, and university research. There is some correlation with weak agencies there, too.