UNDER CISA, DATA WOULD AUTOMATICALLY GET SHARED WITH AGENCIES WITH WORSE CYBERPREPAREDNESS THAN OPM

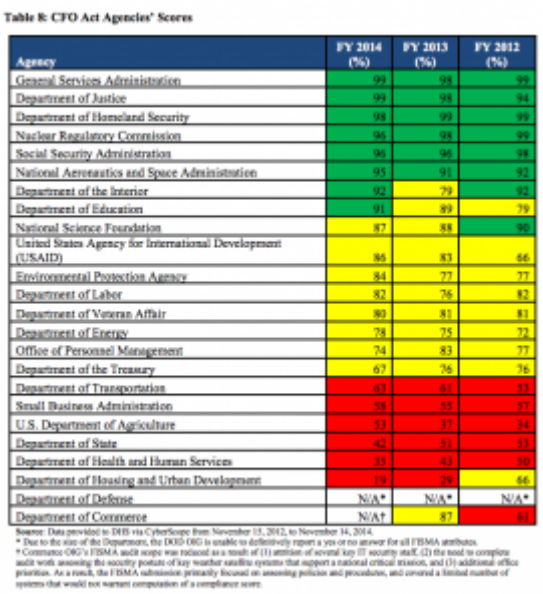

Table 8: CFO Act Agencies' Scores

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	63	53
Small Business Administration	58	55	57
U.S. Department of Agriculture	53	37	34
Department of State	42	53	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.

In the wake of the OPM hack, Congress is preparing to *do something!!!* Unfortunately, that "something" will be to pass the Cyber Information Sharing Act, which not only wouldn't have helped prevent the OPM hack, but comes with its own problems.

To understand why it is such a bad idea to pass CISA just to appear to be doing something in response to OPM, compare this table from this year's Federal Information Security Management report with the list of agencies that will automatically get the data turned over to the Federal government if CISA passes.

> (A) The Department of Commerce.
>
> (B) The Department of Defense.
>
> (C) The Department of Energy.
>
> (D) The Department of Homeland Security.
>
> (E) The Department of Justice.

> (F) The Department of the Treasury.
>
> (G) The Office of the Director of National Intelligence.

So not only will information automatically go to DOJ, DHS, and DOD — all of which fulfill the information security measures reviewed by Office of Management and Budget — but it would also go to Department of Energy, which scores just a few points better than OPM, Department of Commerce, which was improving but lost some IT people and so couldn't be graded last year, and Department of Treasury, which scores *worse* than OPM.

Which is just one of the reasons why CISA is a stupid idea.

Some folks have put together this really cool tool that will help you *fax* the Senate (a tool they might understand) so you can explain how dumb passing CISA would be. Try it!