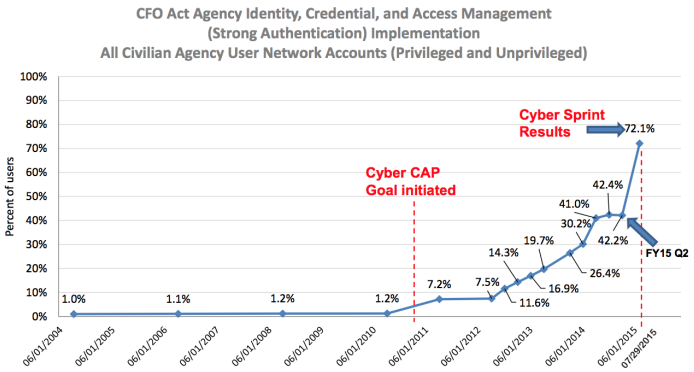
DEPARTMENT OF ENERGY: CYBERSPRINTING BACKWARDS

Earlier this week, I noted that of the seven agencies that would automatically get cybersecurity data shared under the Cyber Information Sharing Act, several had similar or even worse cyberpreparedness than the Office of Personnel Management, from which China stole entire databases of information on our cleared personnel.

To make that argument, I used data from the FISMA report released in February. Since then — or rather, since the revelation of the OPM hack — the Administration has been pushing a "30 day sprint" to try to close the gaping holes in our security.

Yesterday, the government's Chief Information Officer, Tony Scott, released a blog post and the actual results, bragging about significant improvement.

And there have been significant results (though note, the 30 day sprint turned into a 60 day middle distance run), particularly from OPM, Interior (which hosted OPM's databases), and — two of those CISA data sharing agencies — DHS and Treasury.



Whoa! Check out that spike! Congratulations to those who worked hard to make this improvement.

But when you look at the underlying data, things aren't so rosy.

CFO Act Agency*	Identity, Credential, and Access Management (Strong Authentication)								
	All Users			Privileged Users			Unprivileged Users		
	FY 15 Q2 (4/15)	Cyber Sprint Results	Change +/-	FY 15 Q2 (4/15)	Cyber Sprint Results	Change +/-	FY 15 Q2 (4/15)	Cyber Sprint Results	Change +/-
GSA	94	99	+5	0	96	+96	99	99	0
OPM	42	97	+56	100	100	0	41	97	+56
DOT	32	97	+65	67	100	+33	32	97	+65
DHS	87	90	+3	41	97	+56	88	90	+2
Interior	43	89	+46	21	100	+79	45	88	+43
Commerce	77	88	+11	97	93	-4	76	88	+12
Treasury	63	88	+24	3	99	+96	66	87	+21
NSF	59	86	+26	51	99	+48	60	85	+25
HHS	76	84	+8	43	96	+53	78	83	+5
SSA	83	83	0	99	99	0	82	82	0
DOD	87	82	-5	38	58	+20	88	83	-5
VA	10	81	+71	0	100	+100	10	80	+70
EPA	56	80	+23	0	96	+96	61	77	+16
NRC	0	78	+78	0	84	+84	0	78	+78
NASA	0	66	+66	0	55	+55	0	66	+66
Labor	0	65	+65	0	68	+68	0	65	+65
ED	71	57	-14	14	11	-3	76	77	+1
HUD	0	46	+46	0	86	+86	0	45	+45
SBA	0	44	+44	0	63	+63	0	43	+43
USDA	15	35	+20	6	69	+63	15	33	+18
Justice	36	31	-5	26	83	+57	36	30	-6
State	3	28	+25	21	76	+55	2	26	+24
USAID	19	23	+4	0	100	+100	20	21	+1
Energy	32	12	-20	8	13	+5	34	11	-23

* Agencies are sorted based on Cyber Sprint All User Results

We are apparently supposed to be thrilled that DOD now requires strong authentication for 58% of its privileged users (people like Edward Snowden), up 20% from the earlier 38%. Far more of DOD's unprivileged users (people like Chelsea Manning?) – 83% – are required to use strong authentication, but that number declined from a previous 88%.

More remarkable, however, is that during a ~~30 day~~ 60 day sprint to plug major holes, the Department of Energy also backslid, with strong authentication going from 34% to 11%. Admittedly, more of DoE's privileged users must use strong authentication, but only 13% total.

DOJ (at least FBI and probably through them other parts of DOJ will receive this CISA information), too, backslid overall, though with a huge improvement for privileged users. And Commerce (another CISA recipient agency) also had a small regression for privileged users.

There may be explanations for this, such as that

someone is being moved from a less effective two-factor program to a better one.

But it does trouble me that an agency as central to our national security as Department of Energy is regressing even during a period of concerted focus.