

WHAT ARE THE DNC HACK(S) RATED ON OBAMA'S NEW CYBER-ORANGE ALERT SYSTEM?

Yesterday, President Obama rolled out yet another new cyber-directive, this one aiming to better coordinate response to attacks. (PPD, annex, fact

Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>
Level 0 <i>Baseline</i> (White)	<i>Unsubstantiated or inconsequential event.</i>

sheet) Along with all that, the White House released a guideline on the ranking of cyberattacks, including the Orange Alert type table that reminds me of Tom Ridge's discredited system.

I'm going to post at more length about this prioritization system and the PPD.

But for the moment I wanted to post the table separately to ask what you think the DNC hack(s) (remember there were two) would rank on the system. My guess is the initial hack (APT29, alleged to be FSB) would be Level 1 or even 0. State actors spy on political parties all the time, and that's all we've been told APT29 was doing.

The real question is APT28, which is the hack alleged to have ties to Guccifer and therefore to the Wikileaks posting of all the emails. It's

not yet clear the hack was intended to elect Trump (assuming it is Russian); I think it more likely to be retaliation for the Ukrainian coup. It's not clear how important it will be on the election (and I expect more damaging documents to be released closer to the election). And it's not clear how much this *really* has affected public confidence.

The question is still more problematic if you try to grade the OPM hack, which has to be far closer to a Level 4 (because of the risk it placed clearance holders under). But do you also lump it in with, say, the hack of Anthem, which is understood to be related?

I will ask the White House tomorrow if it has ranked the DNC hack(s). But for now, where do you think it would rate?