Hill Prep Document – SASC Cybersecurity Subcommittee

LOEs

- The Task Force is currently focused across four primary lines of effort (no particular order).
- First, we need to protect the DIB
- Second, we need to protect the Research and Development Enterprise, which includes DoD Labs, UARCs, FFRDCs, etc.
- Third, we need to increasingly block malicious foreign investment in and acquisition of our critical technologies. This involves aggressive use of CFIUS/FIRRMA, export controls, and other authorities.
- Finally, we need to use our law enforcement, counterintelligence, and other authorities to disrupt and deny adversaries, to include cyber threat actors regularly targeting our technology.

TOP TEN

- Obviously those four lines of effort are expansive and broad.
- So, in line with the SD's guidance to take action and achieve wins, we've identified 10 specific objectives to achieve over next two years.
- Not in priority order…

1. Operationalize the Critical Programs & Technology list to drive DoD protection efforts

- We currently have a CTL (good thing), mandated by 2019 NDAA
- Next step—operationalize the list; drive DoD protection efforts for our critical technologies/programs
- For example, easy to say AI is important or critical, but need to understand which specific programs are informed by this technology to ensure they're protected to the appropriate standard.
- F-35 (operated by 3 services); need to ensure consistent protection across services
- Fundamental to all our efforts and a big rock that this task force is taking on

2. Increase cybersecurity in the DIB

- First step--ensure the DFARS clause in all new contracts (mandates compliance w/110 NIST CS controls)
- Next step is to ensure compliance with the clause
- Recent DOD IG audit validated that DIB companies are not compliant in general
- Can't be trust-based only
- In short term, DOD teams will visit companies to assess compliance—resource intensive/not scalable
- Longer term, third party certifiers will assess compliance
- Need to ensure standards are applied throughout the entire supply chain
- Current NIST stds not sufficient to defend against APTs
    - Rev 2 in works, which will be applied against critical technology pgms.

3. Incorporate security into source selection and program evaluation criteria

- Often described as "security as 4th pillar" of acquisition
- Cost, schedule and performance not enough, but these are what PMs are graded against
- Security is the new normal—it's expected, and we shouldn't pay more for it
- Needs to be in contractor's business interest to take security seriously

4. Screen & vet individuals working on DoD funded research

- As stated earlier, one of our LOEs is focused on the R&D enterprise
- We know that the Chinese are sending thousands of spies to US colleges
- As Andrew Lelling, the U.S. attorney for Massachusetts, said. "This isn't about targeting everyone who's a Chinese national. But there are thousands who are directly linked to a state-sponsored effort to steal intellectual property."
- Given the threat that's out there, it's perfectly reasonable that the Department wants to know who is actually conducting the research it is funding
- We are currently running a pilot with six universities to explore the best way to gather the names of all those with access / participating in DoD-funded research and screen them
- This pilot will help us design a new policy for the Department

5. Counter adversary talent recruitment programs that target DoD critical technologies

- Talent recruitment is a massive issue—and a main line of effort for the Chinese who are running over 200 different talent recruitment programs
- It's also a major issue for universities who have shared with us how many of their professors they've discovered are members of foreign talent programs
- Recently unveiled a policy that requires grant recipients disclose all their sources of funding which add transparency and help us understand where there are problems

6. Scale use of CFIUS, IEEPA, and other authorities to block adversary acquisition and investment

- DoD is co-leading on **all** Ch CFIUS cases; 52% of all cases
- We need to nominate considerably more problematic cases to Treasury, Commerce or State
- Any additions from Dave Stapleton

7. **Ensure DoD critical technologies are covered under export controls**

- The task force is just starting to unpack this one, but we need to ensure our critical technologies have the appropriate protections in place; controlling exports is a part of that.
- We will work with Commerce and State, the regulatory authorities, to chart the way forward

8. Undermine adversary trust in exfiltrated data

- Can only build our walls so high—can't defend our way out of this
- We need to impose costs by using platforms that obfuscate our data

9. Operationally respond to threat actors

- Again, can't defend our way out of this problem; we're looking at ways to be more proactive and compete below the level of armed conflict like our adversaries are doing to us
- This potentially includes collaboration between CYBERCOM, the CI community and other traditional military capabilities

10. Expose Chinese theft of critical technologies

- Finally, we're thinking thru how best to raise awareness of overall threat with a public information campaign
- We need to educate the public and the communities being targeted by the Chinese—from researchers at universities and experts of all kinds to business professionals and start-ups in Silicon Valley—and make sure that they are aware of the threat they face. We will never be able to police this issue – we need the targets themselves to see the threat clearly so they can be more diligent and thorough when deciding who to work with