Responses to QFRs from the
Subcommittee on Oversight and Investigations
Oversight Hearing
1324 Longworth House Office Building
June 7, 2023
2:00p.m.

Oversight Hearing titled *"Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State Sponsored Cyber Actors"*

From Mr. Dean Cheng, Senior Advisor, China Program, United States Institute of Peace

Questions from Representative Paul Gosar

Q1:

Is there anything stopping the Department of the Interior from allocating a greater percentage of its existing budget to cybersecurity initiatives?

Response:

There may be issues of reallocation of money within a budget, and whether Congressional authorizations allow such reallocations. For example, it may be that money cannot be shifted from, say, Bureau of Land Management to Department of the Interior (DOI) information services without prior authorization.

More importantly, however, is even within the DOI's information services budget, how money is programmed. More money spent on cybersecurity will almost certainly mean less money spent on some other aspect of information management and information services within the DOI. It may mean fewer updates of the web-site, or a lagging purchase of new computers. So long as the information technology/information services budget is (relatively) fixed, additional tasks will be a matter of "robbing Peter to pay Paul."

One consideration, however, may be to determine better metrics of information security, in order to assess the effectiveness of dollars spent on information security. How well is DOI currently doing in terms of securing its information systems?

Questions from Representative Paul Gosar

Q2:

How can DOI better prioritize cybersecurity initiatives within its existing budget?

Response:

Measuring effectiveness and determining efficiency of cyber security is extremely difficult to measure, because it is essentially assessing dogs that do not bark. For example, how does one assess effectiveness of deterrence measures, other than “no war occurred”?

Assessing cybersecurity initiative measure effectiveness might be facilitated by conducting “tiger team” or “red team” attacks. Indeed, this might provide USCYBERCOM with an opportunity to engage in cross-departmental cooperation by staging “attacks” against DOI. Alternatively, asking USCYBERCOM to help assess threats and security capacity of DOI’s information security would potentially help both departments improve their level of operation.

Question from Representative Grijalva

Q1:

In May 2023, a Chinese Government hacking group successfully launched a malware attack on telecommunications systems in Guam and other parts of the United States. What were the consequences of this breach and what can we learn from it to strengthen our cybersecurity posture, especially in the Indo-Pacific region.

Response:

I believe several lessons have emerged.

--One of the most basic is that the same cybersecurity threat groups are often given different names by different cyber-security firms, making it harder to assess how extensively the threat entity has operated, where it has performed prior penetrations, etc. The group "Volt Typhoon" is also known as "Bronze Silhouette" among other names. Encouraging cyber-security firms to not only share data (they often do), but to either use the same nomenclature would improve overall security by facilitating a common understanding of the threat.

--The threat is constantly shifting. "Volt Typhoon" attacks do not require downloading malware, but exploit existing lines of attack. As important, it apparently involves exploiting cyber security firms as an attack pathway.

--There should be little question that the PRC will engage in disruptive attacks against critical infrastructure in time of conflict, and most likely in time of crisis. This is consistent with known People's Liberation Army (PLA) writings, and suggests that policies and courses of action predicated on the assumption that the PRC and PLA will ***not*** conduct such attacks are badly mistaken. It is therefore essential to plan now for both mitigation and response strategies in the likely event of such attacks and ensuing disruptions.