TOPIC: (S//SI//REL TO USA, JPN) Current State of and Proposed Future Cooperation with Japan on SIGINT-enabled Cyber Defense and the development of a Japanese National Cyber workforce

ISSUE: (S//SI//NF) The Government of Japan (GoJ) is undertaking a historic cross-governmental SIGINT-enabled cyber defense initiative and hopes to achieve IOC by April, 2013. Faced with this looming self-imposed deadline, the Japanese are battling constitutional, social, and political impediments to execution. There is considerable friction between forward-leaning elements of the GoJ (such as the Japanese Cabinet Intelligence Research Office (CIRO), the US DNI equivalent) and more conservative elements in the Ministry of Defense (MOD) including the Directorate for SIGINT (DFS) and the Internal Policy Bureau (IB). SUSLAJ believes NSA currently underestimates the pressure the April 2013 deadline is creating for our Japanese SIGINT partners and their resulting desire for immediate progress. The Japanese policy makers' desire for immediate results is leading to decisions that will not likely lead to optimal long-term, national CNO workforce development.

BACKGROUND: (S//SI//REL TO USA, JPN) Based on DIRNSA and D/DIRNSA recommendations for improved USG-GoJ cyber cooperation, the GoJ and the Japanese intelligence community have elevated cyber to a high priority issue. Proposals between DFS and CIRO have advanced rapidly, occasionally generating passionate reactions from Japanese leadership that have surprised NSA. In addition to the efforts by our cryptologic partners there is a GoJ effort to establish a 100-person cyber defense organization, by April 2013. The effort to create a "Japanese Cybercom" is occurring in parallel to, but not in coordination with cooperative efforts to load CIRO or MOD J6 provided signatures as cyber selectors at the joint NSA-DFS FORNSAT site (MALLARD). CIRO, DFS and IB are struggling to develop signature-sharing capabilities and policy between the MOD J6, CIRO, and cyber operators within the new Japanese "Cybercom" organization.

(S//SI//REL TO USA, JPN) DFS and CIRO are currently grappling with an array of concerns: strategic (policy and doctrine), operational (information sharing and workflow), and tactical (technical training) and will not have tenable solutions by April 2013. SUSLAJ is advising all parties on U.S. best practices and assesses that we are beginning to successfully mitigate these concerns, but CIRO and the Japanese Defense Intelligence Headquarters (JDIH), DFS' parent organization, attention remains focused on the short term and providing the GoJ specific cyber-related deliverables by April 2013.

(S//SI//REL TO USA, JPN) SUSLAJ continues to work closely with SID, IAD, NTOC, and FAD to develop both near-term support to and a longer term roadmap for the new Japanese cyber initiatives. Japan provided its first 11 malware signatures to GEN Alexander during a meeting in September with CIRO Director Mr. Kitamura. The signatures were then passed to NTOC for analysis. Seven of the eleven signatures were

not contained in any NTOC repository and were immediately added to those systems in support of cyber defense.

(S//SI//REL TO USA, JPN) Formal agreements are being coordinated to document these efforts. SUSLAJ has presented the DFS with the U.S. Persons Agreement (USP). DFS has agreed in principle but has suggested a few word changes, which are being coordinated. SUSLAJ expects the agreement to be ready for signature in mid-January 2013. The USP will enable increased information sharing. In addition, the first NTOC developed partner cybersecurity MOU is currently being staffed within NSA to allow for the sharing of information assurance sourced cyber data with Japan. This document should be completed by the time DDIR visits Japan.

(S//SI//REL TO USA, JPN) Our Japanese Cryptologic partners have been extremely responsive to SUSLAJ advice and are working diligently to increase sharing and task their SIGINT system. Due to their short-term results oriented focus the Japanese have not paid sufficient attention to the long-term development of a cyber-savvy workforce. SUSLAJ has recently broached this strategic issue with CIRO, JDIH and DFS as a subject that will need to be addressed after achieving IOC for their cyber effort. SUSLAJ is working with ADET to ensure that the Japanese understand the proper concepts of cyber workforce education utilizing concepts adopted by the National Initiative for Cybersecurity Education (NICE) and the Centers of Academic Excellence in Information Assurance (CAEs).

LANDMINES: (S//SI//NF) Avoid any perception of NSA deciding it does not want Japan as a cyber partner. Avoid discussions of which GoJ element will have the cyber lead post IOC, as authorities and community leadership are still being decided.

DEPUTY DIRECTOR'S ROLE: (S//SI//REL TO USA, JPN) Reassure all of the Japanese Cryptologic partners that NSA places great value on our cryptologic relationship and appreciates Japan's contributions. Assure them that NSA understands and appreciates the pressure on JDIH and Japan's deadline pressures and will continue efforts toward future cooperation taking both agencies' and governments' resources and policies into consideration. Encourage continued intra-governmental Japanese cyber cooperation and dialogue. Reaffirm the USG perspective that Cyber is a national concern and that effective CND will need to involve the intelligence community, the armed forces, critical infrastructure, and trusted telecom and technology suppliers. Provide the NSA/NTOC signed MOU to the Japanese for their signature.

ORIGINATOR: (U//FOUO) [redacted], SUSLAJ Chief of Operations [redacted], NTOC, [redacted], 14 January 2013