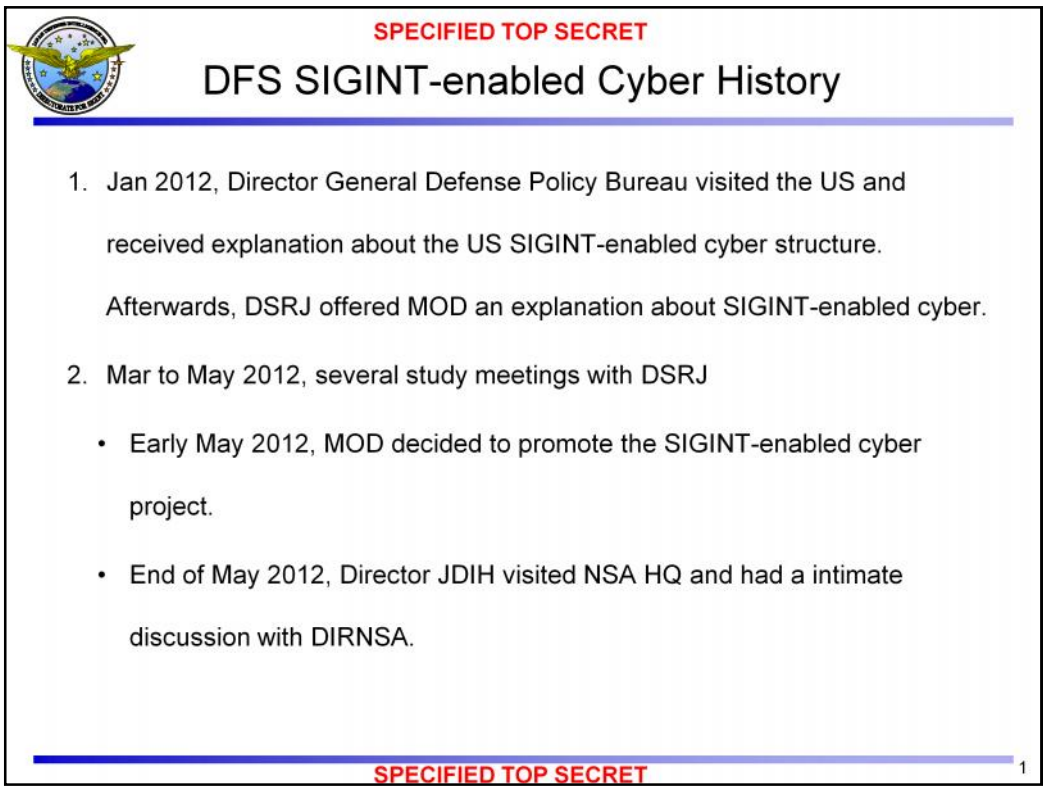
DFS SIGINT-enabled Cyber

February 2013



It is my honor to visit the HQ for the second time and give you a briefing.

I would like to learn a lot about your SIGINT cyber operation and reflect it to DFS future project.

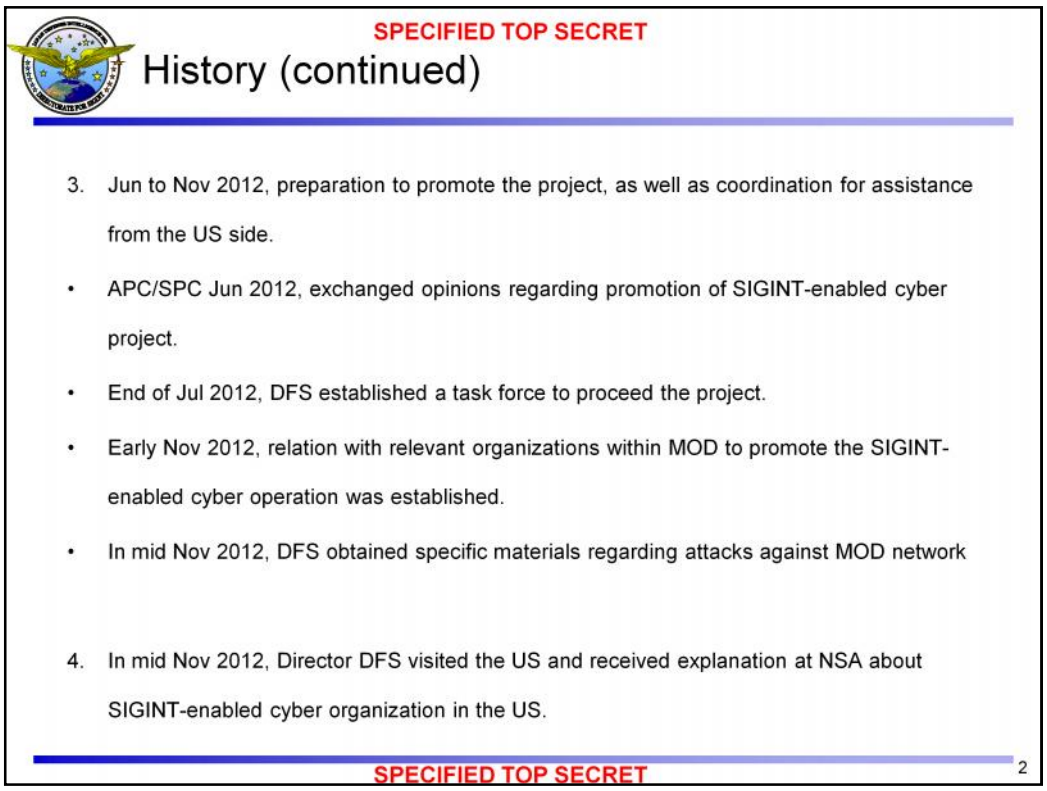
Let me start explanation about DFS SIGINT-enabled cyber operation.

First, I'll talk about the history.

In January 2012, Director General Defense Policy Bureau [redacted] visited the US and received explanation about the US SIGINT-enabled cyber structure. After that, DSRJ offered MOD an explanation about SIGINT-enabled cyber, and MOD and DFS started working on cyber.

Between March and May 2012, several study meetings with DSRJ were held.

In early May 2012, DFS decided to promote the SIGINT-enabled cyber project. At the end of May, [redacted], Director JDIH, visited NSA HQ and had a intimate discussion with GEN Alexander, DIRNSA, and both were aware of necessity to cooperate in SIGINT-enabled cyber operation.



From June to November 2012, we worked on preparation to promote the project, as well as coordination for assistance from the US side.

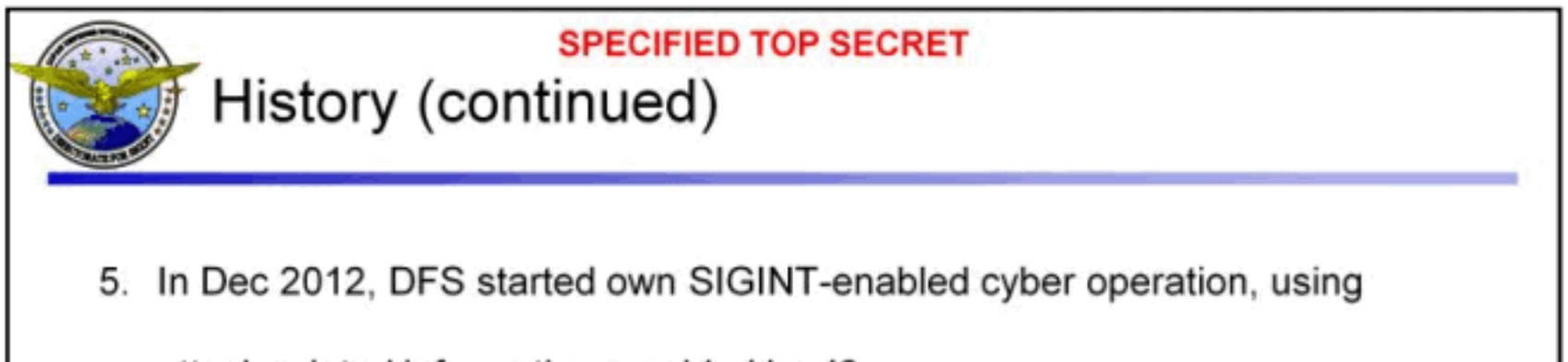
At the APC/SPC June 2012, NSA and DFS exchanged opinions regarding promotion of SIGINT-enabled cyber project in DFS. DFS appreciate the US positive reactions to the Action Items.

At the end of July 2012, DFS established a task force to proceed the project.

In early November 2012, relation with relevant organizations within MOD to promote the SIGINT-enabled cyber operation was established.

Thanks to this relationship, DFS obtained specific materials regarding attacks against MOD network in mid November 2012, and sent them to the US side in order to request advices for collection.

In mid November 2012, [redacted], Director DFS, visited the US and received explanation at NSA about SIGINT-enabled cyber organization in the US, which was of help to consider the future DFS organizational structure.



In December 2012, DFS started own SIGINT-enabled cyber operation, using attack-related information provided by J6.

Initially, in early December 2012, DFS analyzes MALLARD collection with the support from the US side to determine if there is threat information.

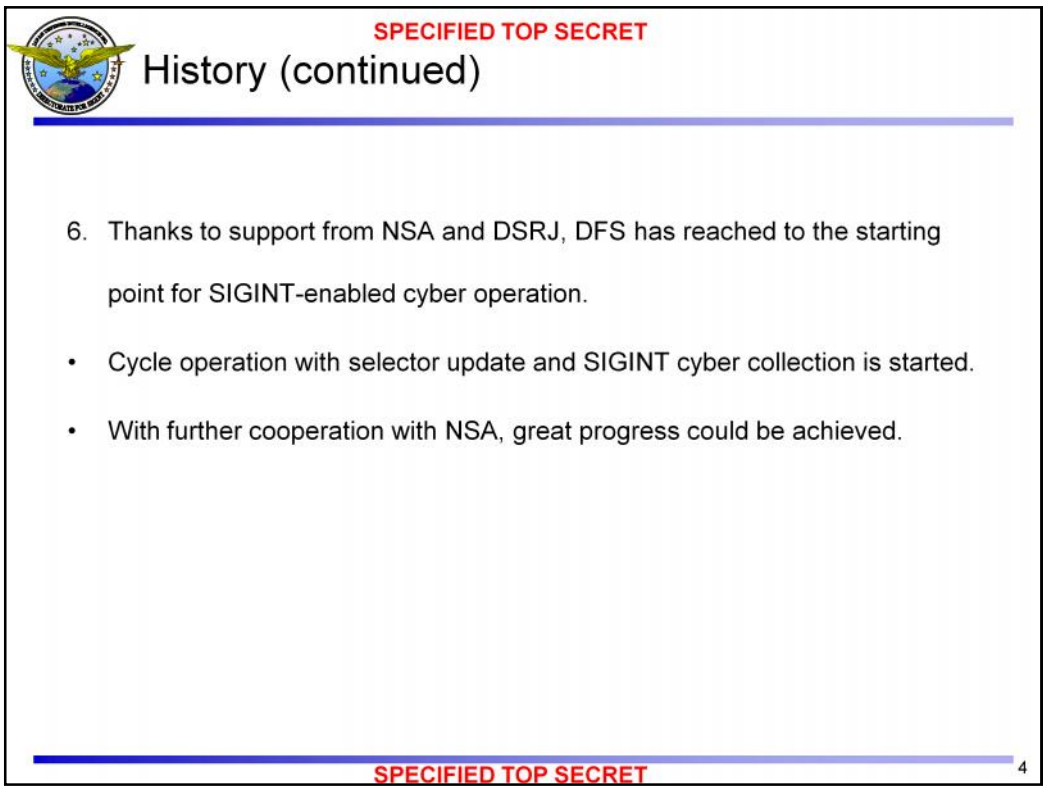
Especially, since the end of December 2012, DFS has a meeting with DSRJ almost every week and received explanation about how specific selectors would be loaded, and is doing collection and analysis.

However, we have not got any hit, probably because sustained targets at MALLARD [redacted] closed networks.

Therefore, DFS asked the US for information about SIGINT-enabled cyber related carriers.

In early January 2013, MALLARD attempted collection against [redacted] which DFS conducted augmented collection when Misawa was damaged by the Northeastern Japan Great Earthquake.

We collected on [redacted] a mail that matched with information from J6 which was a relay information of a mail attacking the MOD network.



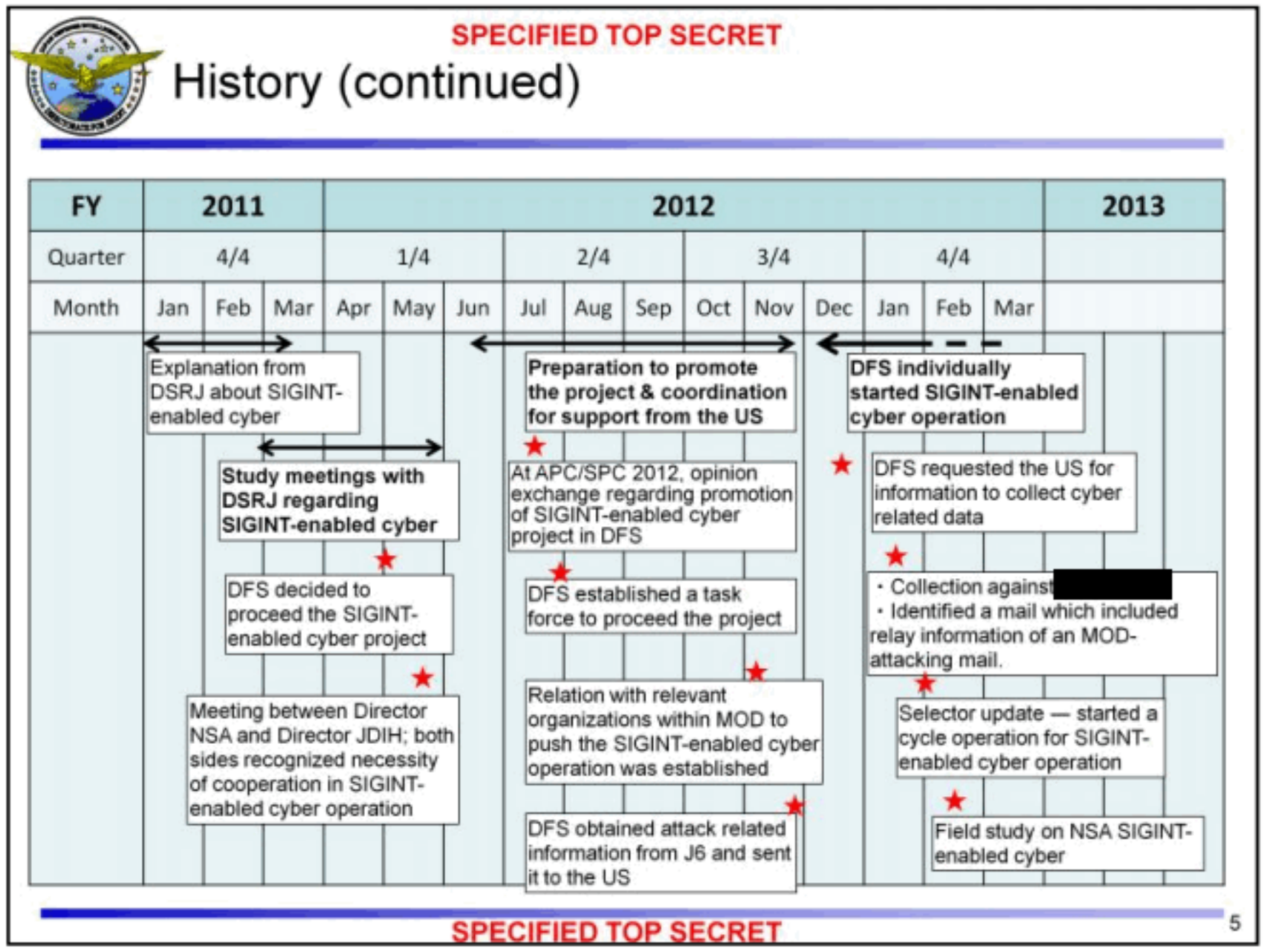
We believe that DFS has reached to the starting point for SIGINT-enabled cyber operation, thanks to NSA's support and in-country effort by DSRJ.

"Cycle operation" with selector update and SIGINT cyber collection has been started.

With further cooperation with NSA, we believe that great progress could be achieved in the future.

SPECIFIED TOP SECRET

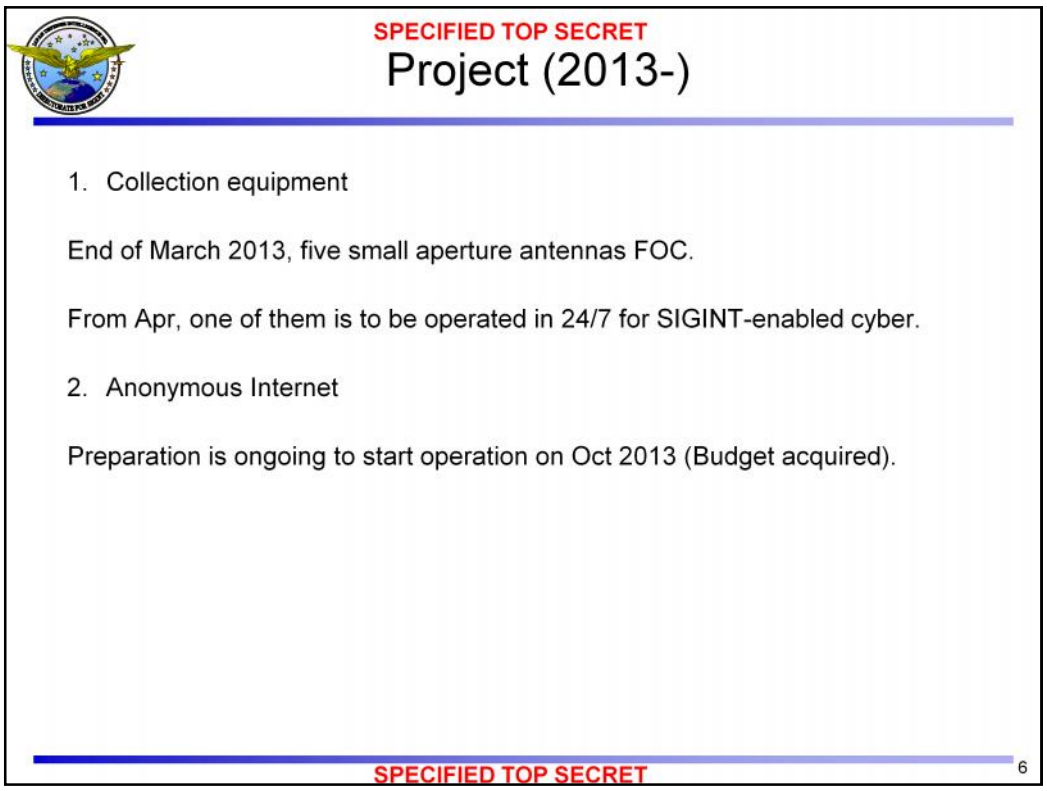
History (continued)



SPECIFIED TOP SECRET

5

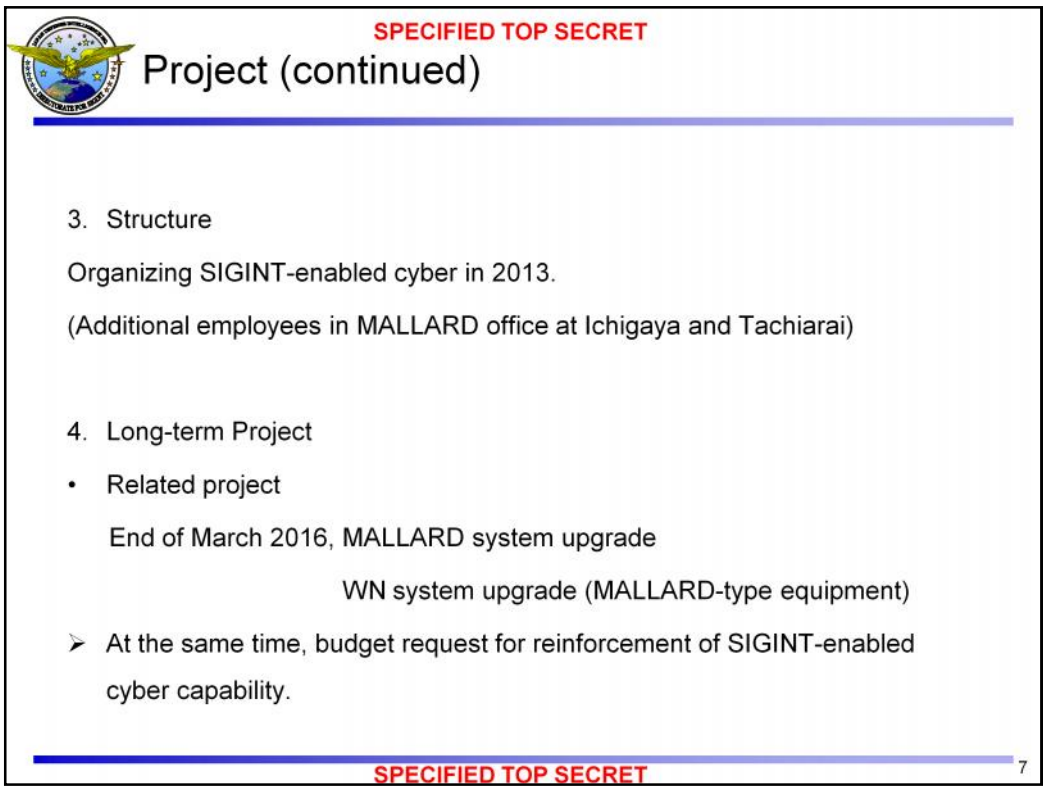
This slide depicts the aforementioned process we have taken so far.



Now, I will explain about our project in and after 2013.

With regard to collection equipment, five small aperture antennas are scheduled to be operational at the end of March 2013. One of them is scheduled to be operated in 24/7 for SIGINT-enabled cyber operation from April.

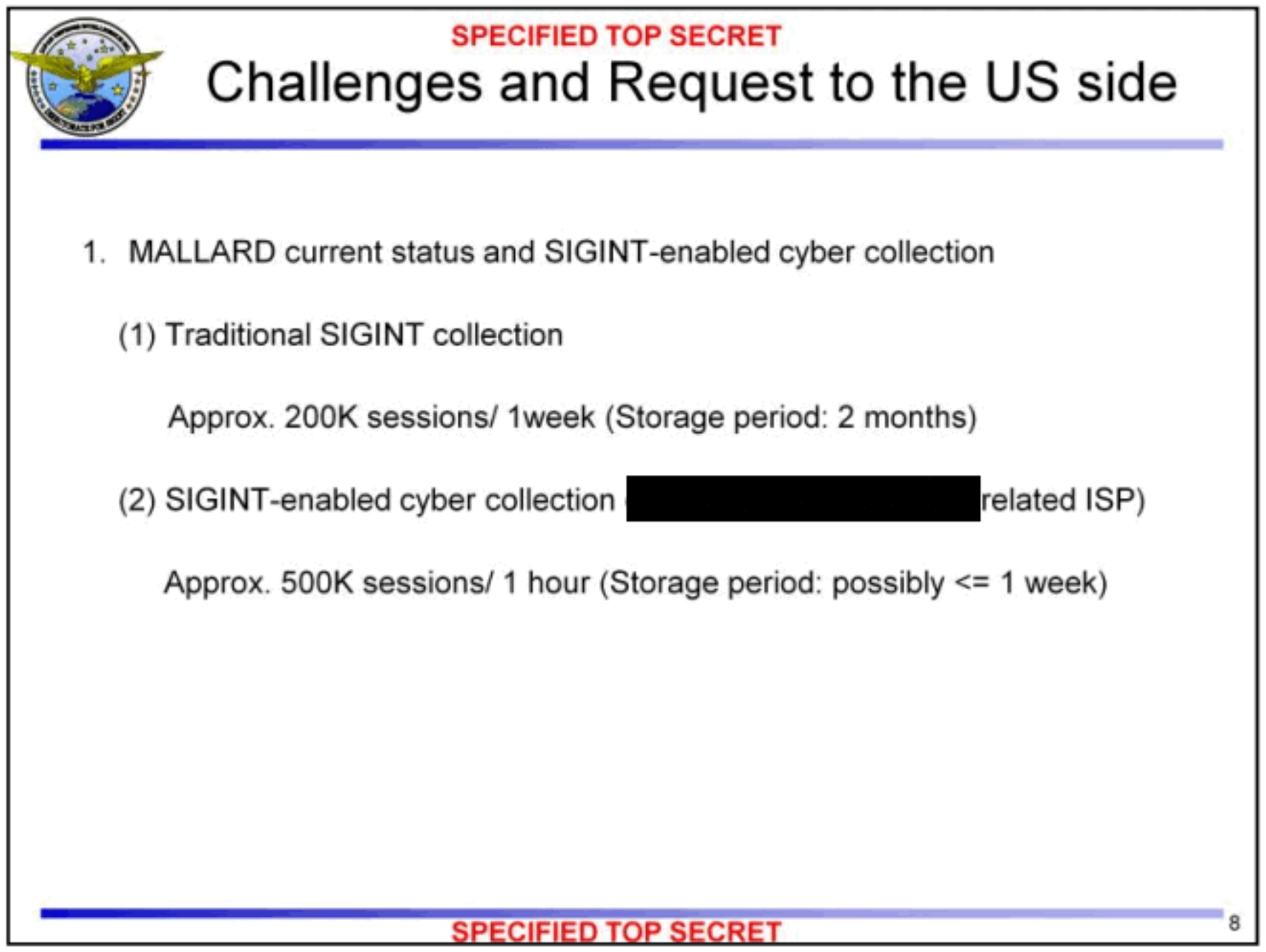
As to anonymous Internet, DFS already acquired budget, and preparation to start operation is ongoing aiming at IOC in October 2013.



Being authorized to organize SIGINT-enabled cyber structure, additional employees are scheduled to be assigned at MALLARD office in Ichigaya and Tachiarai.

In long-term perspective, by the end of March 2016, MALLARD system upgrade as well as WN system upgrade, i.e. introduction of MALLARD type system, are scheduled.

At the same time as these upgrade, we are to make a budget request for reinforcement of SIGINT-enabled cyber capability.



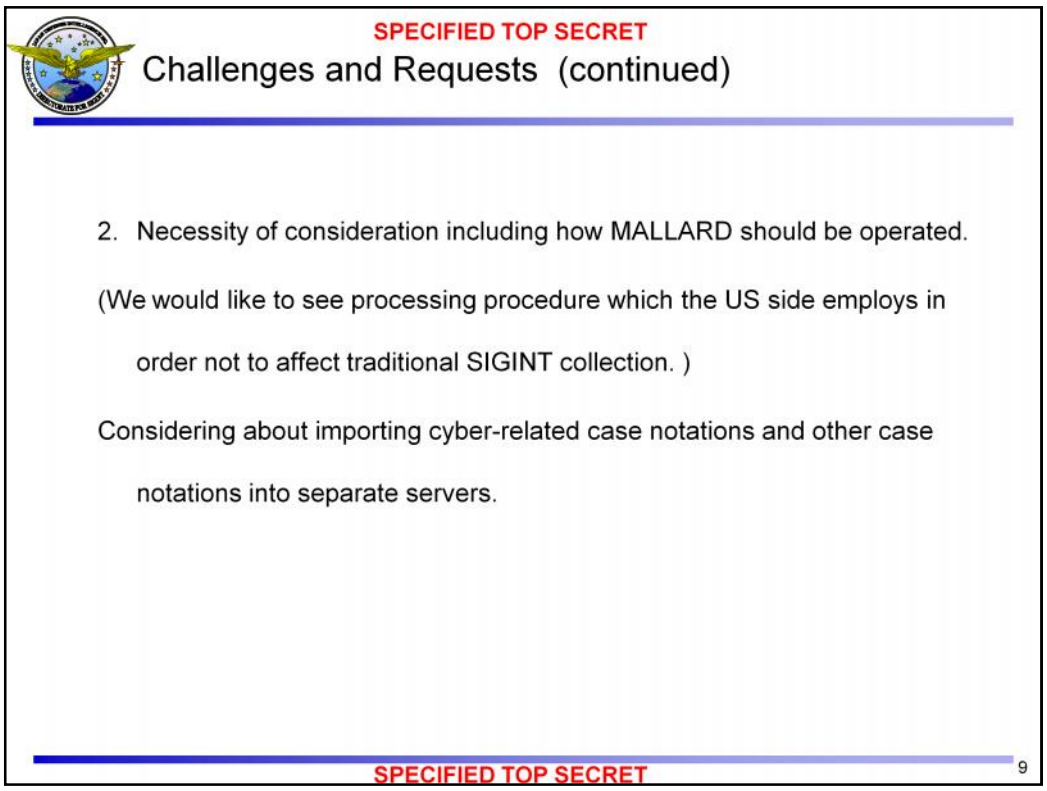
Challenges and request to the US side.

First, MALLARD current status and SIGINT-enabled cyber collection.

MALLARD was originally introduced for traditional SIGINT collection, and is conducting about 200K sessions in a week. Data is saved for approx. two months. As DFS does research and analysis during that period, if preservation time is shortened, it will affect SIGINT operation at DFS.

As I explained in the history, DFS [redacted] ISP carrier on [redacted] to collect SIGINT-enabled cyber data from this January. The number of collected sessions reached to about 500K in one hour. Keeping this pace, MALLARD data storage period might be less than one week.

As it affects our SIGINT operation, we are not able to do sustained collection for SIGINT-enabled cyber.

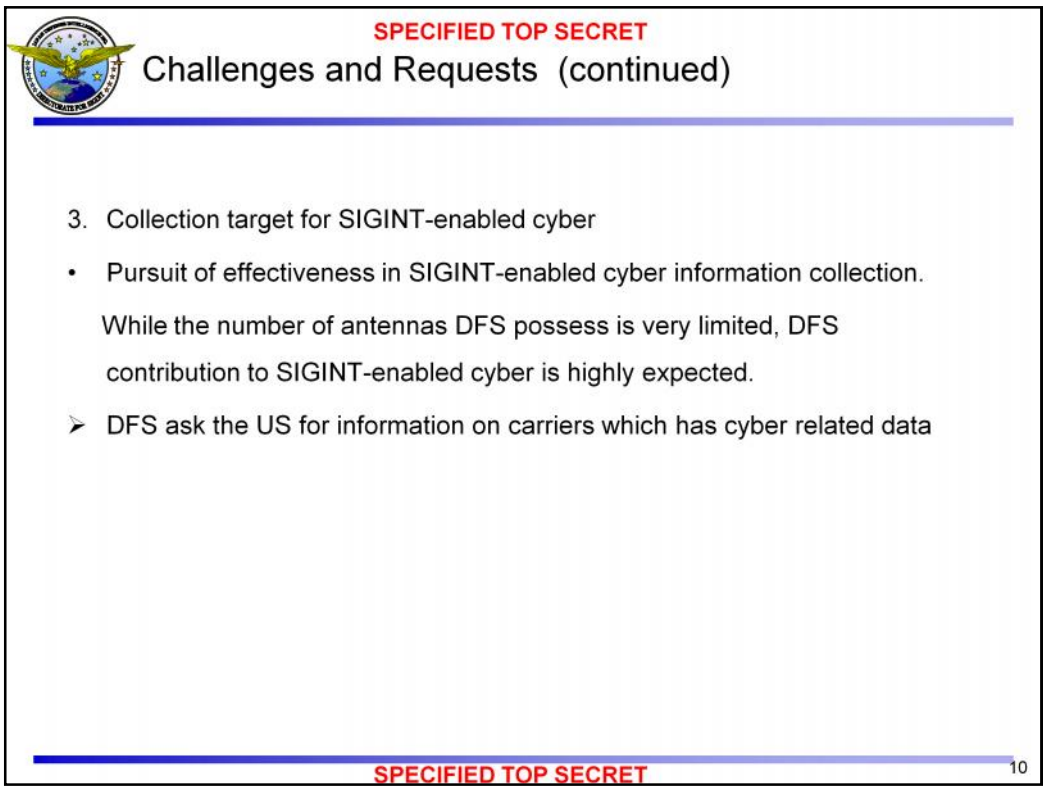


Thus, we are facing necessity of consideration including how MALLARD would be operated.

DFS is considering about importing cyber-related case notations and other case notations into separate servers.

We would like to see processing procedure which the US side employs in order not to affect traditional SIGINT collection, and would appreciate your technical assistance.

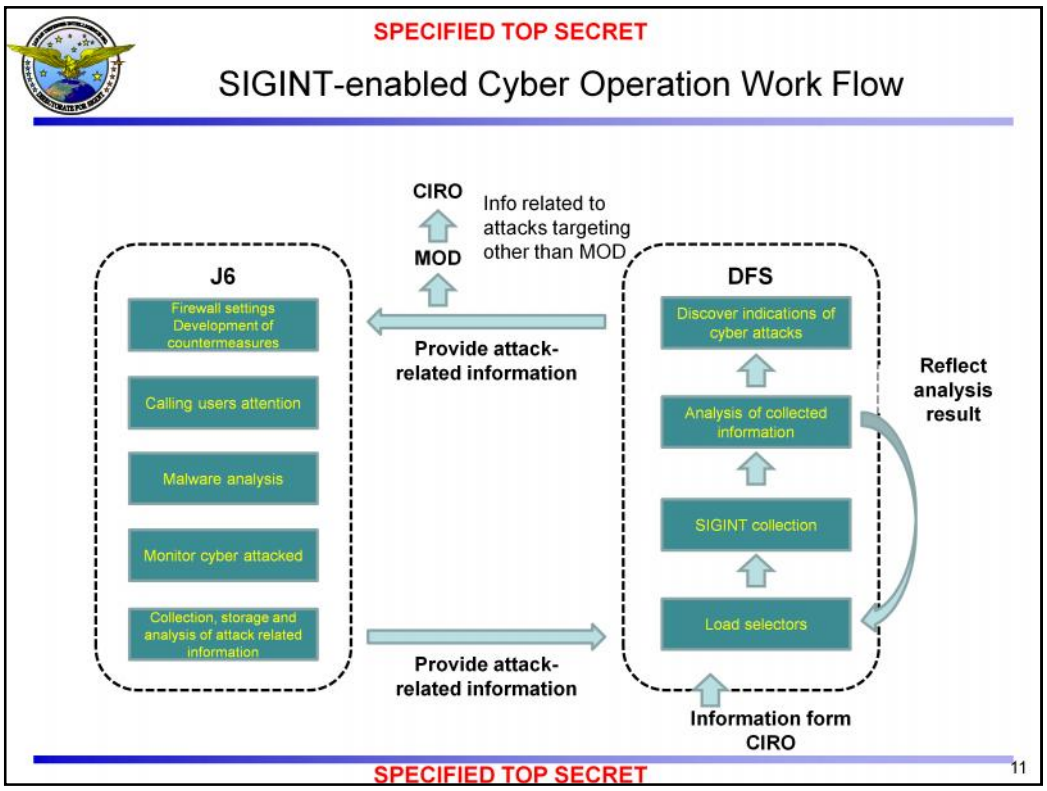
Let me add that we had a meeting with DSRJ last Thursday and they explained about possible solutions further examination. We felt assured and are looking forward solutions.



Regarding collection target for SIGINT-enabled cyber,

While the number of antennas DFS possess is very limited compared to the US, DFS contribution to SIGINT-enabled cyber is highly expected by both inside and outside of DFS.

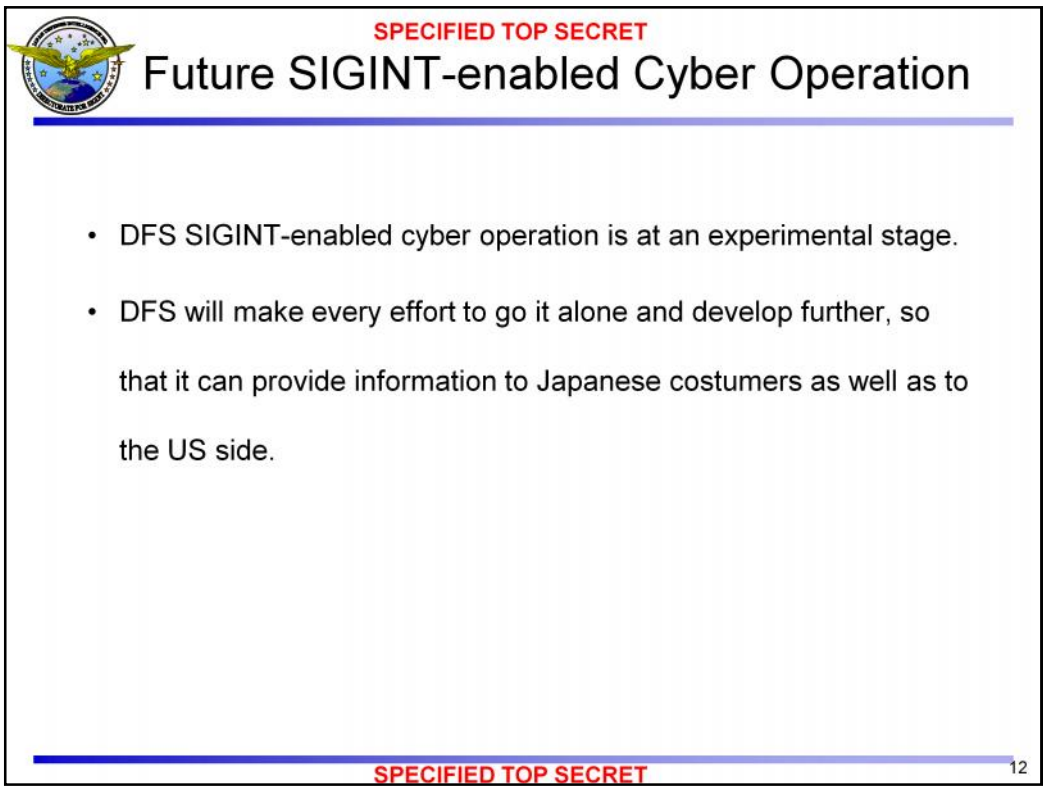
As we need to pursue effectiveness in SIGINT-enabled cyber collection, DFS asked the US for information on carriers which has cyber related data.



DFS SIGINT-enabled cyber operation flow is depicted here.

J6 roles and functions showed in left include our assumptions, because J6 function is not disclosed to us. Their function include refining FW setting, alert users, malware analysis, cyber monitor and collection, storage and analysis of attack related information.

With attack information provided by J6, we load selectors, collect and analyze SIGINT, reflect analysis result to selectors. In this cycle, we hope to discover indications of cyber attack and provide J6 with threat information.



Lastly, future SIGINT-enabled cyber operation.

DFS SIGINT-enabled cyber operation is at an experimental stage.

DFS will make every effort to go it alone and develop further, so that it can provide information to Japanese costumers as well as to the US side.

For the future SIGINT-enabled cyber operation, we would appreciate the US cooperation. Thank you for your kind attention.