(TS//SI//NF) New FAA702 Certification in the Works – Cyber Threat
By [redacted] on 2012-03-23 1423

(TS//SI//NF) NSA has drafted a new FAA702 Certification to target Cyber Threats. It is close to being ready for formal coordination with Department of Justice and the Office of the Director of National Intelligence. If approved by the FISA Court, likely many months from now, the Certification will enable analysts to task selectors to SSO's FAA702 authorized systems (PRISM, STORMBREW, OAKSTAR, FAIRVIEW, BLARNEY) which do not fit into one of the current Certifications for Foreign Intelligence. This will be of great benefit to NTOC because it will fill a targeting gap – some cyber threat actors are currently targeted under the existing Certifications when the actor is known and can be tied to a foreign government or terrorist organization. However, many cyber threat targets currently cannot be tasked to FAA702 due to lack of attribution to a foreign government or terrorist organization. The new certification will not require this attribution, and rather only require that a selector be tied to malicious cyber activity. The FAA702 collection will then be used to determine attribution, as well as perform collection against known targets.

(TS//SI//NF) The Certification will also for the first time spell out the authorization for targeting cyber signatures such as IP addresses, strings of computer code, and similar non-email or phone number-based selectors. Although the current Certifications already allow for the tasking of these cyber signatures, NSA and its FAA702 overseers (e.g. – Dept. of Justice; ODNI) have yet to reach a common understanding as to how this unique type of targeting and collection will be implemented. This new Certification will help to codify the FISA Court's guidance on targeting using the signatures listed above. SSO's "upstream" FAA702 accesses will perform collection against all signature types and are poised to make immediate significant contributions. The PRISM access will be used primarily for e-mail and similar selector types. Taken together, SSO's FAA702 collection will fill a huge collection gap against cyber threats to the nation, and the approval of this new Certification is one of the DIRNSAs highest priorities.

POCs: [redacted] PRISM Mission Program Manager, S3531, [redacted] SSO Cyber Lead, S3531; [redacted]