



Some Key (SSO) Cyber Milestone Dates Since Fall 2005

- 2006 – DNI Processing = [REDACTED] @ 622 Mbps.
- Spring (?) 2007 – Comprehensive National Cybersecurity Initiative Firms-Up.
- Spring 2007 – TURBULENCE/NCC & the First C&O [REDACTED] Take Shape.
- August 2007 – Protect America Act; CT, only. [REDACTED] WC2 @ 2.5 Gbps.
- Spring 2008 – CNCI FYDP Becomes Real.
- July 2008 – FISA Amendments Act; CT Cert, first, Foreign Governments Cert in Sept.
- March 2009 – FAA Cert C, Counter-Proliferation. TURMOIL T16 @ 2.5 Gbps.
- March 2010 – [REDACTED] briefs SSO on [REDACTED] FAA Cert A Case.
- Summer 2010 – TURMOIL XNET @ 10 Gbps.
- September 2010 – [REDACTED] Activates XKEYSCORE Deep Dive.
- 2010 to 2011 - Low-Profile TURMOIL @ 10 Gbps deployed worldwide.
- Spring 2011 – NCSC/SSO Activate Content Collection @ US-3140/MADCAPOCELOT.
- June 2011 – US-3171 DANCINGOASIS. (Need I see more?)
- August 2011 – NIPF Band A Cybersecurity Becomes Cyber Threats to US Infrastructures.
- January 2012 – President Obama Reconfirms the Transit Program.
- May 2012 – Dept. of Justice approves targeting certain signatures under FAA FG Cert.
- May 2012 – First TURMOIL BLUESNORT content activation for FAA [REDACTED]
- July 2012 – Dept. of Justice approves targeting certain IP addresses under FAA.
- August 2012 – Iranian DDoS attack against Saudi Aramco.
- December 2012 – FAA of 2008 extended until December 31, 2017.
- [REDACTED]

(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]
[REDACTED] SSO Cyber Lead, S3531; [REDACTED]



(TS//SI//NF) **What's Next**



- Plan to add Dropbox as PRISM provider
- Want to add Cyber Threat Certification
- Expand collection services from existing providers
- Change UTT tasking system to allow tasking of phone numbers and sending one selector to multiple providers



(TS//SI//NF) Conclusion *What to Remember*



- PRISM is one of the most valuable, unique, and productive accesses for NSA – don't miss out on your targets.
- Recommend tasking ***all*** DNI and DNR selectors to FAA 702 if they meet the criteria. Your target's communications could be flowing through SSO's accesses which **only FAA can access**. Communications paths constantly change.
- Recommend **using Rules-Based-Tasking in UTT** to ensure that both PRISM and passive/upstream SSO FAA accesses are given the selectors.
- Some Product Lines do not use PRISM and other SSO accesses optimally. They are **missing unique collection** on their targets.
- FAA 702 collection = PRISM program providers + FAA Upstream SSO programs with access to **thousands** of non-PRISM internet domains, DNR collection, cyber signatures and I.P. addresses.

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO SIGINT DIR	EXREG CONTROL NUMBER 2012-704	KCC CONTROL NUMBER S353-113-11
THRU	ACTION	
SUBJECT (S//REL) SSO's Support to the FBI for Implementation of their Cyber FISA Orders	<input checked="" type="checkbox"/> APPROVAL	EXREG SUSPENSE
	<input type="checkbox"/> SIGNATURE	KCC SUSPENSE
	<input type="checkbox"/> INFORMATION	ELEMENT SUSPENSE
DISTRIBUTION V2, V3, V07		
SUMMARY		

RECOMMENDATION: (U//FOUO) Approve the provision of the assistance to FBI, with the proviso that the FBI remains responsible for any additional expenses incurred.

PURPOSE: (S//REL) To obtain the SIGINT Director's approval for the Office of Special Source Operations (SSO) to provide ongoing technical assistance to the Federal Bureau of Investigation (FBI) for the implementation of the various orders they have obtained, and will obtain, from the Foreign Intelligence Surveillance Court (FISC) in certain Cyber cases involving agents of foreign powers (e.g. - [REDACTED])

[REDACTED] soon, [REDACTED]). The preparation of this Staff Processing Form was a collaborative effort between SSO and the NSA Office of General Counsel (OGC).

BACKGROUND: (S//REL) On December 20, 2011, NSA received a request for technical assistance from the FBI seeking access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers. The FISC has issued a number of orders at the request of the FBI authorizing electronic surveillance directed at communications related to computer intrusions being conducted by foreign powers. The orders include some that are limited to pen register/trap and trace (PRTT) information as well as others that authorize collection of content. The first of these for which NSA assistance has been requested is directed at communications related to intrusions conducted by the [REDACTED] (Docket Number 11-91), regarding what FBI refers to as STYGLIAN FLOW.

(S//REL) In mid-2011, prior to receipt of the request for technical assistance, SSO became aware of FBI's plans to seek these orders and has been in discussions with FBI throughout the latter half of the year, in the belief that use of NSA's collection/processing infrastructure would allow the FBI to

Continued...

COORDINATION/APPROVAL					
OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
OGC	/email/30-Jan.				
FIB	/email/19 Feb.		S3	/s/ 3-20-12	
SI	/s/		S35		
NTOC	/s/		SV		6/31 Jan.
T	/s/ 6 Feb.		POC		
ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED		
[REDACTED]	S353	[REDACTED]	20111221		

FORM A679BDE REV NOV 2008(Supersedes A6796 FEB 05 which is obsolete)
NSN: 7540-FM-001-5465

SECURITY CLASSIFICATION

Derived From: NSA/CSS Manual 1-52

Dated: 8 January 2007

SECRET//REL TO USA, FVEY

Declassify On: 20320108

SECURITY CLASSIFICATION**Page 2 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders**

maximize the value of the collection without incurring the expenses associated with duplication of that infrastructure. Although FBI conducts numerous electronic surveillances without NSA's assistance, the vast majority of them are directed against targets located inside the United States, and U.S. providers served with FISC orders are ordinarily able to identify and deliver to the FBI most, if not all, of the targets' communications that they carry. That is because such electronic surveillance is typically effected at a point or points in the provider's infrastructure in physical proximity to the target's location. In the case of computer intrusions being conducted by foreign powers, the providers may be carrying a target's communications, but it is much more difficult to identify and locate them, because the communications in question will enter and leave the United States via any convenient path, and their path may be obscured to avoid detection. In other words, in these cases, because the target's location is outside the United States and not well-characterized, effecting the surveillance via FBI's traditional means is not effective.

(S//REL) However, in support of FAA and in anticipation of the need to conduct similar collection activities for computer network defense purposes, over the last decade, NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States. Collection at such chokepoints is much better suited to electronic surveillance directed at targets located outside the United States than FBI's traditional means of collection. In theory, FBI could rely on the orders it has obtained to direct U.S. providers to conduct surveillance at these chokepoints without relying on NSA capabilities, but it would take a considerable amount of time to do so, and FBI would have to reimburse the providers to recreate (i.e., duplicate) what NSA has already put in place. The cost alone would be prohibitive, and the time lost in doing so would necessarily result in a loss of foreign intelligence.

(S//REL) The assistance being sought by the FBI is limited in nature. The U.S. providers served with Secondary Orders in this matter will assume full responsibility for the provisioning of PR/TT and content collection to the FBI. Since all of the authorized "facilities" (typically known as "targeted selectors" in NSA parlance) to date are Internet Protocol (IP) addresses used by the targets, there is no question as to the providers' abilities to employ devices under their control (e.g., routers) to provision fully-compliant, authorized intercept.

(S//REL) Neither the providers nor the FBI will require NSA's Government off the Shelf (GOTS) Digital Network Intelligence (DNI) collection and processing solutions (e.g., TURMOIL, XKEYSCORE). Instead, metadata and full content derived from the authorized intercept will be produced using Commercial off the Shelf (COTS) processing solutions. If these COTS processing solutions involve components developed at NSA's expense and used, primarily, for NSA's Cyber survey purposes, the SSO will make careful and informed decisions prior to authorizing use of these components.

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

Page 3 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders

(S//REL) Prior to authorizing use of the extensive secure Wide Area Networks established at the two primary providers (cover terms, LITHIUM and ARTIFICE, respectively) as the end-to-end data delivery infrastructure to connect intercept and processing locations with the FBI's designated Cyber data repository at the Engineering Research Facility, Quantico, VA, SSO will make careful and informed decisions to ensure this capability is undertaken on a 100% non-interference basis with NSA's current and future data backhaul needs on these same networks.

(S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

(S//REL) Should the FBI require a sustained and high-level of dedicated analytical resources (i.e., cleared, technical manpower) at the providers in order to optimize the collection effectiveness of their PR/TT and content orders, they will contract for those services directly with the providers. If, on the other hand, the FBI's requirement for provider analytical support is more ad hoc and aperiodic in nature during the period of time these orders remain in effect, SSO will make careful and informed decisions prior to authorizing labor charges against the relevant SSO contracts with the providers for these services on behalf of the FBI. Any charges that cannot be justified as necessary for NSA purposes will not be made unless/until FBI agrees to reimburse NSA.

DISCUSSION: (S//REL) If SID decides to approve the requested assistance, SSO will assist the FBI in effecting any cyber orders submitted to it after the NSA/OGC has verified that each of them contains language permitting NSA's involvement. As stated in Attachment 1, NSA will have the opportunity to review and respond to any proposed use of FISA-derived information from these collections prior to the Attorney General authorizing the use of such information in any criminal proceedings.

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA

Continued...

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

Page 4 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA Amendments Act (FAA) of 2008. To the contrary, the relatively recent discovery of these FBI Cyber FISA orders and the countless pages of SIGINT-derived evidence that was cited in the respective Applications to the FISC have already formed the basis for a dialog between NSA's OGC and the Department of Justice's National Security Division.

(C) DIRECTOR, SIGNALS INTELLIGENCE DECISION:

CONCUR: Jeffrey H. Howard DATE: 3 - 8 27-12

NON-CONCUR: _____ DATE: _____

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

(U//FOUO) CNO LEGAL AUTHORITIES



Office of General Counsel

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Objectives for Today's Brief

- Overview of SIGINT law
- Overview of Information Assurance Law
- What do I need to know?
- How do I apply this Stuff to what I'm doing?

Classification: SECRET//COMINT//Rel 4
EYES//20291123

(U//FOUO) Helpful Questions

- **What authorities are being used to collect the information that I'm looking at?**
- **Where is this information being collected?**
 - SIGINT platforms? - Tutelage sensors? –Collateral Source?
- **Who will receive access to the collected information?**
- **What retention and dissemination restrictions apply to the collected information**
 - (e.g., SIGINT Procedures, Service Provider Rules, etc.)?

Classification: SECRET//COMINT//Rel 4
EYES//20291123

The Importance of “Purpose”

The purpose governs the restrictions imposed upon the collection.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

If they get nothing else out of the briefing, they need to know and remember that SIGINT is collected for FI/CI/SMO (FI) purposes and they must apply the SIGINT (FI) rules (FISA and USSID SP0018) to all raw SIGINT and IAD collection is done for system/data security purposes and they must apply (for now, though IAD is coming up with their own procedures like USSID 18) DoD regulation 5240.1-R and the rules to stay within the Wiretap Act Service Provider exception. COMSEC collection by JCMA is typically done for security purposes and follows National Telecomms and Info Systems Security Directive (NTISSD) 600.

(U) Key Authorities & Restrictions

- United States Constitution
- Executive Order 12333, “U.S. Intelligence Activities”
- NSC Intelligence Directive 6, “Signals Intelligence”
- National Security Directive 42, “National Policy for the Security of National Security Telecommunications & Information Systems”
- Title III of the Omnibus Crime Control Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (18 U.S.C Sections 2511-2521, 2701-2711) – “Federal Wiretap Act”
- Foreign Intelligence Surveillance Act (FISA) as amended by the FISA Amendments Act (FAA)
- Other Federal laws
- DoD Regulation 5240.1-R and USSID SP0018

Classification: SECRET//COMINT//Rel 4
EYES//20291123

NSA/CSS (NTOC and ANO) were not given any additional authorities. The idea is to use the same authorities more effectively and take advantage of the same expertise (analytical and technical) that is used to defend and exploit.

(U) U.S. Constitution

Article II (Power)

“The President shall be Commander in Chief of the Army and Navy...” and conducts foreign affairs.



Classification: SECRET//COMINT//Rel 4
EYES//20291123

Article II power not unlimited.

(U) Executive Order 12333

"United States Intelligence Activities," dated December 4, 1981 (as amended by E.O. 13284 (2003), 13355 (2004) and 13470 (2008))

- SECDEF, in coordination with DNI, is executive agent for SIGINT. See Section 1.10(e).
- DIRNSA is the functional manager for SIGINT. See Section 1.3(b)(12)(A)(i).
- DIRNSA is the National Manager for National Security Systems, and is responsible to SECDEF and DNI. See Section 1.7(c)(6).
- **No other department or agency may conduct signals intelligence activities, except as otherwise delegated by the SECDEF, after coordination with DNI. See Section 1.7(c)(2).**
- Collection done in accordance with procedures approved by the Attorney General. See Section 2.4. – USSID 18
- Assist Law Enforcement and other Civil Authorities. See Section 2.6.

Classification:TOP SECRET//COMINT//Rel 4

The collection done by NSA/CSS, electronic surveillance and using monitoring devices, requires procedures. Procedures established by the head of the IC element and approved by the AG, after consultation with the DNI must protect constitutional and other legal rights and limit use to lawful governmental purposes.

Assist LE and other Civil authorities. NSA/CSS has procedures in place to provide assistance. These procedures provide protection of NSA resources, equities, sources and methods.

Differentiate Reporting for lead purposes and use for LE. For instance, disseminate SIGINT to FBI re the fact that a foreign intruder is in a US system; FBI may start their own investigation (which could start as a FI/CI investigation because believe to be foreign before turning to a criminal investigation.)

If the SIGINT system incidentally collected a US hacker conducting intrusion activities, give to OGC who will have to report a potential violation of US law (The Computer Fraud and Abuse Act.) Also, SIGINT must avoid any further collection of that US person hacker

From IAD side, can provide threat reports or OGC can report a violation of law to FBI or the CI units of the military for investigation if an intrusion is seen in the DoD systems. IAD could not assist without a request for technical assistance (and a warrant from the FBI/CI units) if a specific DoD system user is under investigation.

Authority to conduct CNE

- (S) EO 12333 assigns NSA the Signals Intelligence (SIGINT) Mission, which includes COMINT and in turn CNE.
- (U) CNE evolved as a natural transition of the foreign intelligence collection mission of SIGINT. As communications moved from telex to computers and switches, NSA pursued those same communications.
- (U) 2 type of CNE activities:
 - (U) Collection Activities- designed to acquire foreign intelligence information from the target computer system.
 - (S) Enabling Activities- designed to obtain or facilitate access to the target computer system for possible later CNA, or force use of alternate communication systems.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

CNE has evolved as a natural transition of the foreign intelligence collection mission of SIGINT. COMINT mission includes CNE.

Two types of CNE activities: the collection of FI, CI, SMO information and enabling activities that allow access. Collections activities are those designed to acquire foreign intelligence information from the target computer system and enabling activities are those activities designed to obtain or facilitate access to the target computer system.

Constitution Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

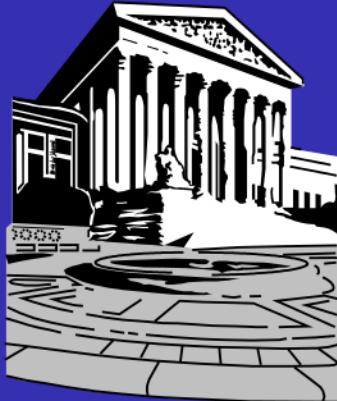
UNCLASSIFIED

Classification: SECRET//COMINT//Rel 4

EYES//20291123

Applies to SID and IAD. Purpose is to protect USPs from unreasonable searches and seizures by the USG and NSA/CSS employees, contractors and military or Agents of the Government. Can go over the fact that in ones personal life, a person can do whatever s/he likes unless there is a law against it. In contrast, the USG is only allowed to do what it is authorized to do.

Supreme Court Cases



- *Olmstead v. U.S.*
(1928)
- *Katz v. U.S.*
(1967)

Classification: SECRET//COMINT//Rel 4
EYES//20291123
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Prior to '67, Gov could surveil/intercept comms as long as didn't make physical intrusion into constitutionally protected area (e.g. home)

Describe cases.

Electronic Surveillance

Supreme Court rules ELSUR is a search and seizure under the 4th Amendment to the U.S. Constitution...Depending upon...

How it's done.

Where it's done.

Against whom it's done.

Why it's done.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Electronic Surveillance History

- *Privacy rights developed in case law*
- *Court determines electronic surveillance is a search and seizure under the 4th Amendment*
- *Statute passed in 1968 (Omnibus Crimes Control and Safe Streets Act—the Wiretap Act)*
- *Scope*

Purpose was to give LE procedures to allow Electronic Surveillance for Law Enforcement purposes

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Congress also knew intelligence agencies and government required to do ES for FI and Comsec purposes. Service providers needed to do surveillance of their own systems. More exceptions written into the law.

(U) Federal Wiretap Act

- Crime to intentionally intercept or endeavor to intercept or procure any other person to intercept any wire, oral, or electronic communication.
- Crime to intentionally use or disclose or endeavor to use or disclose to any other person the contents of any wire, oral, or electronic communication if they know or have reason to know that the interception violated federal law.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Fed statute starts by saying it is illegal.

(U) WIRETAP EXCEPTIONS

- Interception for foreign intelligence purposes permissible if conducted in accordance with Foreign Intelligence Surveillance Act and/or other applicable procedures.
- Interception with prior consent of one party to the intercepted communication is OK under federal statute but be aware of state two-party consent statutes if acting in private capacity.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

-Will talk about the FI exception when briefing SIGINT rules

-Consent-for IA and FI. Scope of consent matters. Drives expectation of privacy. (But see Long case.) Also, the DoD system consent banners do not mean that there is consent for NSA SIGINT to start looking at DoD systems for FI purposes. ***Need SIGINT consent BEFORE tasking any US identifier, to include DoD, as a single selector for SIGINT system collection.*** SIGINT consent is two fold: 1. the actual consent, and 2. approval of the FI/CI/SMO purpose of the consensual SIGINT collection by Dir/DDir.***

For Soaring Eagle, NSA has SIGINT consent from STRATCOM Commander for the DoD NIPRNET and SIPRNET systems and data. NSA has SIGINT consent from DIA for JWICS systems and data.

Service Providers-providers need to see if email got to the right place. Make sure bandwidth being used properly, not being stolen etc. Are limited to purpose. Once a target is identified and there is another purpose (e.g. CI or LE) talk to OGC.

Trespassers-used when a service provider asks another service provider for information on an intruder one hop out. Can view trespasser info for LE, intel, system protect purposes. 4 requirements: need system owner permission; act under color of law; only trespasser's comms, not legit user; stop when investigation purpose done.

(U) WIRETAP EXCEPTIONS

- COMSEC Monitoring by US Government personnel is permissible if conducted in accordance with Attorney General-approved procedures (see NTISSD No. 600).
- Service providers may intercept or monitor communications on their systems
 - 1) to ensure the systems are functioning properly or
 - 2) to protect their rights or property in their systems.
- Trespasser exception

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

-Will talk about the FI exception when briefing SIGINT rules

-Consent-for IA and FI. Scope of consent matters. Drives expectation of privacy. (But see Long case.) Also, the DoD system consent banners do not mean that there is consent for NSA SIGINT to start looking at DoD systems for FI purposes. ***Need SIGINT consent BEFORE tasking any US identifier, to include DoD, as a single selector for SIGINT system collection.*** SIGINT consent is two fold: 1. the actual consent, and 2. approval of the FI/CI/SMO purpose of the consensual SIGINT collection by Dir/DDir.***

For Soaring Eagle, NSA has SIGINT consent from STRATCOM Commander for the DoD NIPRNET and SIPRNET systems and data. NSA has SIGINT consent from DIA for JWICS systems and data.

Service Providers-providers need to see if email got to the right place. Make sure bandwidth being used properly, not being stolen etc. Are limited to purpose. Once a target is identified and there is another purpose (e.g. CI or LE) talk to OGC.

Trespassers-used when a service provider asks another service provider for information on an intruder one hop out. Can view trespasser info for LE, intel, system protect purposes. 4 requirements: need system owner permission; act under color of law; only trespasser's comms, not legit user; stop when investigation purpose done.

Other Federal Laws

- *Computer Fraud and Abuse Act*
 - *Illegal to obtain unauthorized access or exceed authorized access to any protected computer.*
 - *Does not apply if generally available to the public using legitimate knowledge/tools/services.*
 - *If going beyond what is publicly available, it is considered CNE and USSID DA3655 and all SIGINT rules apply.*
 - *There is an FI exception to the law and a trespasser exception similar to surveillance law.*
 - *Includes non-communications data.*
 - *NSA/CSS non-attribution, covered accounts are for open source research, not CNE (NSA Policy 6-6) Eliciting information w/o disclosure of gov affiliation is not allowed.*
 - *mission-related research at home is an OPSEC concern*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

- Line between open source and unauthorized access a fine one sometimes.
E.g. facebook pages only available to friends and family are not publicly available etc. Can also use an analogy-if don't lock door, doesn't mean it is an invitation for intruders to come in. If a default password is being used by a less than competent Sys Admin type, it still would not be publicly available.
- Be aware if using info only gained from SIGINT or other special collection to access/monitor US systems, often will not be publicly available.
- If going beyond authorized access for FI purpose, SIGINT rules, to include FISA law, and TAO USSID applies. F4, monitoring device on computers in the U.S. applies.
- If doing stuff at home, outside the scope of employment, may be subject to the federal law (no exceptions apply).
- NSA was granted authority from the President to collect not only COMINT but any other data at rest on a foreign target computer while conducting out CNE missions. (Also have a delegation from SECDEF for room audio and video.)
- Open source policy: Eliciting info while under cover has undisclosed participation issues and Privacy Act issues; even some open source research is not done from home for opsec concerns. Have uncovered and covered accounts for publicly available info research.

Intel Community History

- *Church/Pike Commissions investigate Intelligence Community*
- *Abuses of power found*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Describe Shamrock, Watchlisting, narcotics collection.

Computer Security Act '87. EO 12333 gave DIRNSA the comsec mission for the fed government. Congress concerned that an intel agency had authority over traditional civilian agencies (with personal information like the social security administration, the IRS etc) so Congress passed the CSA and gave the developing standards and guidelines for the security of non-national security systems to Commerce's National Institute of Standards and Technology (NIST). Gave NSA authority over national security systems.

SIGINT
*Congressional Inquiries into the IC
Church/Pike Committees Found*

*SIGINT information TO, FROM, and
ABOUT U.S. Citizens was:*

Improperly Collected

Improperly Retained

Improperly Disseminated

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Look at USSID SP0018. There is a section on Collection, retention, dissemination. If in compliance with USSID, are in compliance with 4th amendment in each of these activities.

Committee Findings and Results of Investigations



- *Termination of illegal collection activities*
- *Executive Order requiring the establishment of procedures relating to U.S. person information*
- *Greater Executive and Legislative Oversight*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Congressional/Executive Response to IC Abuses

- *Federal Law* → *Foreign Intelligence Surveillance Act*
- *Executive Order* → *E.O. 12333 Intelligence Activities*
- *Regulations and Procedures* → *DOD 5240.1-R and USSID SP0018 Minimization Procedures*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

FISA only applies to the FI/SIGINT collection.

DoD rules incorporated into USSID SP0018 which is supposed to be the working document.

Core SIGINT authority From EO 12333

- *To collect, process, analyze, produce, and disseminate signals intelligence information and data to support national and departmental missions and for:
- foreign intelligence;
- counterintelligence; or
- the conduct of military operations.*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

All the front end selectors and queries on SIGINT raw traffic databases are based on FI/CI/SMO requirements given to NSA by DNI or secdef. The National Intelligence Priorities Framework. SIGINT committee validates the requirements. Info Needs from NSA/CSS customers based on SIGINT requirements and clarify the broader SIGINT requirements.

Change in the E.O. 12333 allows the IC agencies to take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the US. See Section 1.1(f)

This probably applies to both SIGINT and IA information but NSA would still not typically disseminate directly to those entities, due to classification law and requirements and protection of sources and methods (mainly from the SIGINT side). A cut-out fed gov agency can help sanitize the information. Sanitization is different than the “minimization” procedures that are required. The latter is for protection of sources and methods, the latter for protection of USP information privacy rights.

SIGINT Targeting/Collection

- (S//SI//REL) NSA has "core" authority to intentionally target the following:
 - (a) Non-U.S. Persons,
 - (b) who are located overseas,
 - (c) for the purpose of collecting
 - Foreign Intelligence,
 - Counter Intelligence and
 - Support to Military Operations information (FI purposes).

Classification: SECRET//COMINT//Rel 4
EYES//20291123

**REMEMBER if it's SIGINT
rules/procedures: USSID SP0018**

Purpose is to balance . . .

*The Government's need for foreign intelligence information
with
Individual Privacy Rights*

In a way that is . . . Specific enough to be useful

*But not so specific so that each new technology
renders it obsolete*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

SIGINT Targeting Specific Communicants

USSID SP0018 Section 4

The Four Rules

- *Foreign Persons outside the U.S. of FI/CI/SMO interest -- fair game*
- *No Foreign Persons in the U.S. (unless diplomatically-immune and using passive collection) must have Attorney General approval*
- *No U.S. Persons in the U.S. without a Court Order*
- *No U.S. Persons outside the U.S. without Court Order*

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

It is the communicant that matters. Do you have a foreign communicant overseas? If you have foreign hacker using a US computer, NTOC/ANO can develop selection strategy to collect the foreign hackers comms using a US computer similar to targeting, for instance, badguy@us_service_provider.com. Equipment does not have expectation of privacy. NTOC/ANO may use a US IP address in conjunction with a selector that will collect only the foreign intruder's comms on, not any legitimate USP user of, that US computer. May not intentionally target a known USP communicants in the US.

Contrast: May query on US IP address in BLUESASH/TUTELAGE for system protection mission but may not query on a US IP address as straight hit in SIGINT. Will get legit users of the US computer with that IP address.

Can query/select in the SIGINT collection, foreign IP addresses found in Bluesash.

Same technology looks for intrusion signatures in Bluesash/Tutelage and SIGINT. Can share technology. (e.g. masterworks is SIGINT collection technology called Cynecs when deployed to Bluesash sites. Strickler (Sigint Tickler)/Tickler the same.)

-If making federated queries, the most restrictive (SIGINT) rules apply. Therefore, data repositories must keep data sourced so that analysts know what procedures to apply to the data but also so that analysts can make queries on just Bluesash/Tutelage (least restrictive), just SIGINT or on both. Keep data sourced (e.g. arcsight has the data color coded by source) so that analysts know which procedures to apply to which data. SIGINT procedures must be applied to SIGINT data; IA procedures to the IA data.

Targeting Issues



Presumptions

(If no other information is available)

- *In the U.S., then U.S. person*
- *Outside the U.S., then foreigner*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

E.g. all that is known is that the hacker came from/through a Pakistani ISP.
Presume is foreign.

If all that is known is that the intrusion is from a US ISP, then presume is a USP.

SIGINT Targeting Issues



U.S. Person Information

- *INTENTIONAL (need additional authority)*
- *INADVERTENT (Did not know U.S. Person)*
- *INCIDENTAL (Legitimate foreign target; acquire U.S. Person information/communications)*
- *REVERSE (Target foreign entity to intentionally acquire U.S. Person information/communications)*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

-No targeting/collecting/disseminating a USP communication without additional authority.

-If used a presumption, and you find out you have been targeting/collecting/disseminating communications to/from/about a USP, then must stop collection (or get the correct authority), cancel reports, and report in the IG quarterly.

-Incidental collection, then apply the dissemination procedures.

-Cannot target a foreign entity just to acquire USP communications. When targeting the foreign hacker and using a US IP address in conjunction with the foreign hacker signature, that is not reverse targeting. Your collection is focused on the foreign hacker communications, what the foreign hacker is doing and what data the foreign hacker is stealing. There are no legitimate USP comms and it is impossible to know what or whose data the foreign hacker is exfiltrating.

US Government Communications

- Communications to or from any officer or employee of the US Government, or any state or local government may not be intentionally intercepted and must be destroyed upon recognition.
- Exception to the destruction requirement include anomalies that reveal a potential vulnerability to US communications security. Get a destruction waiver and authority to disseminate the US person information.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

If there is no legitimate USG communicant, there is no USG communications.
That is different than collecting a foreign intruder stealing a bunch of USG information. All that USG information is incidental.

USSID SP0018 5.4.c. and d. Other exceptions include: Significant foreign intelligence or evidence of a crime or threat of death or serious bodily harm to any person.

This section also talks about USP to USP communications and US-US communications destruction requirements.

US Government Communications

- If a foreign intruder is just using a US computer and is not communicating with any legitimate US Government official or employee, it is not considered to be US Government communications; report following dissemination procedures.
- Socially engineered emails to US Government employees or officials ARE US Government communications.

Classification:SECRET//COMINT//Rel 4
EYES//20291123

Targeting by Subject Matter USSID SP0018, Section 5

*Applies to the use of selection terms to
INTERCEPT communications on the
basis of CONTENT, not necessarily on
the basis of the IDENTITY of the
communicants*

*Covered in the “Processing” Section of
USSID SP0018*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

E.g. hacker signatures. Hacker signatures pull in a lot. Focus on foreign target use of intrusion capabilities. Defeat out any USP use of the hacker signature. Worst thing NTOC could do is to turn the SIGINT system to collect against a USP hacker. It is not FI/CI, basically doing surveillance for LE purpose without warrant. If incidentally collect information on USP hacking into a protected computer, this is a violation of law that should be reported to DL violations for OGC to refer. Do not want to see any/many of these.

Targeting by Subject Matter USSID SP0018, Section 5

*No selection terms that are reasonably likely
to intercept or have intercepted
U.S. person communications
UNLESS
there is reason to believe that
Foreign Intelligence will be obtained*

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Targeting by Subject Matter
USSID SP0018, Section 5

*Selection terms that
have intercepted or are likely to intercept
U.S. Person communications
MUST BE DESIGNED
(to the greatest extent practicable under the
circumstances)
to DEFEAT communications
that do not contain foreign intelligence*

Classification: SECRET//COMINT//Ref4

EYES//20291123

Pay attention to what is being collected. NSA has a positive responsibility to defeat out to the extent possible collection of USP comms.

(S) SIGINT Dissemination Procedures (USSID SP0018, Section 7)

- Incidental USP information in valid collection, apply “minimization” procedures
- “Minimization” means, prior to disseminating any information obtained through SIGINT collection, evaluate information for foreign intelligence and decide if any incidentally acquired US person information is suitable for dissemination.
- The information to, from, or about a USP must be necessary to understand the FI or assess its meaning in order to not minimize.

Classification: SECRET//REL 4
EYES//20291123

-Can query in Bluesash/Tutelage on IP address seen in SIGINT without it being a dissemination of the SIGINT raw traffic. If decide to task that US IP address in Bluesash/Tutelage (I.e. on the deny list) then it is a dissemination of a US identity and must get SIGINT dissem approval.

NTOC has upfront dissemination authority for intrusions into .mil/.gov systems. Need to alert JTF-GNO, DISA, the network owner of intrusions in a timely manner and the IP addresses intruded into are necessary to understanding the intell

**(S) SIGINT Dissemination Procedures
(USSID SP0018, Section 7)**

- If necessary, include the USP information, focusing on the FI, but only disseminate the actual USP identity with appropriate level dissemination authority. (.mil)
- “US Idents in SIGINT” is a good source.

Classification: SECRET//REL 4
EYES//20291123

ACCESS and RETENTION to Raw Traffic containing USP information-USSID SP0018, Section 6

- 5 Years on-line
- up to 10 years off-line—historical searches
- Retention exceptions (SID/DIR determination, tech data, evaluated data)
- E.O. 12333, Section 2.3
- Limited to SIGINT production personnel
- Recognizes intrusiveness of SIGINT
- Maintains SIGINT within community of individuals trained on 4th Amendment Procedures

Classification: SECRET//REL 4
EYES//20291123

FISA Overview



Classification: SECRET//COMINT//Rel 4
EYES//20291123

FISA Definitions U.S. Persons



- *U.S. Citizen*
- *Permanent Resident Alien
(Green Card Holder)*
- *Corporations (incorporated in the U.S.)*
- *Associations (primary membership composed of U.S. persons)*
- *U.S. flagged ships/aircraft (DoD definition)*

Classification: SECRET//COMINT//Rel 4
UNCLASSIFIED//FOR OFFICIAL USE ONLY
EYES//20291123

FISA Definitions Foreign Power



- A *foreign government or any component thereof*
- A *faction of a foreign nation*
- An *entity openly acknowledged to be directed or controlled by a foreign government(s)*
- A *group engaged in international terrorism*
- A *foreign based political organization*

Classification: SECRET//COMINT//Rel 4

EYES//20291123

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FISA Definitions Agent of a foreign power



- *An officer or employee of a foreign power*
- *A spy, terrorist, saboteurs, aider/abettor, or conspirator*

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Classification: SECRET//COMINT//Rel 4
EYES//20291123

e.g. USP hacker not included unless can show state sponsorship. Then get appropriate approval. If a USP is the hacker, it is a law enforcement issue and should be referred to OGC.

Other FI requirements for alien smuggling, narcotics, organized crime, gun running, money laundering are similar. If a USP was involved, NSA/CSS could not target unless working for a foreign power or also a spy, terrorist, saboteur, or aider/abettor/conspirator.

FISA – Restrictions

(S//SI//REL) Federal Law Regulates the collection of foreign intelligence if it falls into 1 of 4 categories of “electronic surveillance:”

1. (F1) Intentional collection of the communications sent by or intended to be received by a particular, known U.S. person who is in the United States.
2. (F2) Wiretaps in the United States.
3. (F3) The acquisition of certain radio communications where all parties to that communication are located in the United States.
4. (F4) Installation and use of a device in the United States for monitoring of information in which a person has a reasonable expectation of privacy.

Classification: SECRET//COMINT//Rel 4

EYES//20291123

UNCLASSIFIED//FOR OFFICIAL USE ONLY

NTOC I believe has a FISA on the [REDACTED] in order to collect [REDACTED] intrusions into the [REDACTED] network.

F4 is where CNE usually falls. Other devices includes accessing/CNE against a computer located in the U.S.

FISA Amendment Act (FAA) of 2008

–H.R. 6304

(S//SI//REL) The FISA Amendment Act was signed into law by President Bush in July 2008.

(S//SI//REL) FAA replaced the Protect America Act (PAA) (*also known as "FISA Modernization"*). PAA was signed into law on Sunday, 5 August 2007, amending the FISA act, for a period of 180 days (until 15 February 2008). PAA Established a standard and set the stage for FAA.

Classification: SECRET//COMINT//Rel 4
EYES//20291123
UNCLASSIFIED//FOR OFFICIAL USE ONLY

FAA

- (S//SI//REL) The new FISA Amendments Act (FAA) modified the FISA to include changes to collection that:
 1. falls into categories 2-4 of “electronic surveillance” and the target is a non-US Person outside the U.S. (collection off a provider,
 2. targets a U.S. Person

(S//SI//REL) FAA is Title VII of the FISA. It includes:

- 702, targeting non USP outside the U.S., collection inside the U.S. with service provider assistance.
- 703, USP outside the U.S., collection inside the U.S. with service provider assistance.
- 704, USP located outside the U.S., collection outside the U.S. without service provider assistance (i.e. E.O. 12333 collection; old 2.5 authority)
- 705, USP with concurrent FISA collection inside the U.S. (705a, i.e. f1 authority) and collection outside the U.S. without service provider assistance (705b, i.e. E.O. 12333 collection; old 2.5 authority).

Classification: SECRET//COMINT//Rel 4

EYES//20291123

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FAA section 702, foreign governments certification: NTOC uses the authority to target [REDACTED] that were attributed to the [REDACTED]
[REDACTED]

NTOC wants another 702 certification to target foreign hackers outside the US for FI purposes. Because attribution is hard, just having to prove foreignness and an FI purpose is especially useful to NTOC. However, the selectors will likely not be the hard/strong selectors DoJ is used to.

SIGINT Targeting Specific Communicants

Foreign Persons outside the U.S. of FI/CI/SMO interest Examples:

1. US -IP address used by itself
2. US – IP in conjunction with an Intrusion Signature
3. DoD - PKI certificates

Classification: SECRET//COMINT//Rel 4
EYES//20291123

1. Request to select based on a foreign hacker signature in conjunction with a DoD military IP address. Nothing seen in SIGINT. The SIGINT system doesn't see everything. Collection architecture has to be in place. So, without asking, analyst put the DoD military IP address in as a straight hit and obtained hundreds of hits.
2. DoD PKI certificates were compromised. In SIGINT without additional authority, may look for revoked DoD certificates because no legitimate DoD person should be using. Can also look for valid certificates only in conjunction with the [REDACTED] signatures so will only collect the [REDACTED] using the certificate (but will not find new uses of [REDACTED] use of the certificates.) May not look for expired certificates because the legitimate DoD person could renew. May not look for valid certificates without obtaining the DoD person's consent.
3. Had incidental collection of an [REDACTED] using an army email address and getting into army systems. May collect against that army email address because had evidence that it was being used by a foreign person outside the US. Reported to the army on the intrusion. Wanted to collect for a short while to see what the foreign target was doing/after. Unfortunately, after two weeks, a legitimate army person also started using that email address. Now we have USG comms.

Information Assurance Legal Framework

- Executive Order 12333 –
 - DIRNSA is the National Manager for National Security Systems, and is responsible to SECDEF and DNI. See Section 1.7(c)(6).
- National Security Directive 42, “National Policy for the Security of National Security Telecommunications & Information Systems”
- DoD Regulation 5240.1-R – Governs collection of USP information by DoD.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

(U) National Security Directive 42

- President designated DIRNSA as the “National Manager” for National Security Telecommunications and Information’s Systems Security.
- Among other things, DIRNSA directed to assess the overall security posture of and disseminate information on threats to and vulnerabilities of national security systems.
- Establishes, *inter alia*, policies and organization to protect national security systems that process:
 - Classified information
 - Intelligence activities
 - Cryptologic activities
 - Command and control
 - Weapon or weapons system
 - Military or intelligence mission, except for systems used for routine administrative and business applications.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

NSS includes unclass systems if involved in intel activities, military or intell missions (includes BLUESASH/TUTELAGE monitoring because includes NIPRNET.) However, NSS does not typically include those systems supporting National Security Systems: Personnel, financing, accounting systems typically not NSSs.

E.g. Centcom commander uses electrical power grid of central Florida. Not a national security system but may look at whether or not has a direct contract with centcom which can bring them under the NSS rubric.

(U) National Security Directive 42 Continued

- Disseminate all-source information on threats to US national security systems. (NSD-42, 7.g.)
- NSA may not monitor NSSs without a request for technical assistance or request for a vulnerability assessment from the system owner. Includes requests for monitoring, red teaming, blue teaming, system forensics.
- If above request made of NSA then must have certification from the system owner that there is a notice and consent policy in place, of the activity must fit within Service Provider rules and IA procedures.
- Requester may put restrictions on the collection/monitoring, access, retention, use or dissemination contained in Ground Rules.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Ground Rules are established between NSA and the requester. NSA/CSS must follow the service provider rules to stay within the exception, DoD regulation 52490.1-R AND the Ground Rules for this activity.

***Work being done for JTF-GNO and also Soaring Eagle is strictly under Service Provider (JCMA still will need a legal cert in order to be legal.)

(U) IA procedures: Service Provider rules and DoD Reg 5240.1-R

- Includes DoD BLUESASH/TUTELAGE & NSA/CSS NISIRT monitoring
- Collection/monitoring/access/disclosure must be consistent with ensuring system functionality or furthering the protection of the service provider's rights and property in their systems/network.
- Is USP information disclosure necessary? DoD 5240.1-R
- Retention of USP information limited (90 days per DoD Regulation 5240.1-R or in accordance with the agreed upon Ground Rules.)

Classification: SECRET//COMINT//Rel 4
EYES//20291123

-NSA is the service provider for NSA net and DOD NIPRNET (AS&W monitoring per DoD Instructions 0-8530.1 and O-8530.2)

-Disclosure of foreign intrusions to SID is fine under the service provider rules. All foreign comms intrusions into DoD are suspect and can be disseminated for SID to help find out attribution, how intrusion works etc.

-Access and dissemination are part of disclosure of the data and must be for ensuring system functionality/protection of the provider's rights and property.

-DoD regulation allows collection/retention of USP information that arises out of a lawful comsec investigation. However, NSA must determine that the USP information fits within that criteria within 90 days.

-**The Ground Rules may have different retention periods.

**IAD Oversight and Compliance policy (IAD Management Directive 20)

(S) Global Defense of US Networks

- IA authorities allow NSA to monitor DoD or other national security systems for indications of malicious activity in response to a request from the system owner, and disseminate that information law procedures.
- The Computer Security Act of 1987 (as amended by the FISMA) requires NIST to collaborate with NSA and does not preclude NSA from providing security support to Federal departments and agencies outside the national security sector. In a Memorandum of Understanding dated March 1989, NIST and NSA agreed that NSA could—upon request by Federal agencies, their contractors, and other government-sponsored entities—conduct assessments of the hostile intelligence threat to Federal information systems, provide technical assistance, and recommend products and solutions to secure systems against the threat.
NSA follows the IA procedures for technical assistance to other agencies

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

-Many players in the CND/cyber security. The difficult managerial task is to make the respective authorities and monitoring systems work well together since, to be effective, network defense has to be efficient and timely.

-Tech assist outside NSSs-Also Executive Order 12333, which was revised in July 2008. Sections 2.6(c) and (d) permit NSA to provide specialized equipment, technical knowledge, and assistance of expert personnel for use by any department or agency and render any other assistance and cooperation to civil authorities not precluded by law. Any provision of assistance of expert personnel must be approved in each case by OGC.

(S) Global Defense of US Networks

- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (signed in January 2008) applies to all Federal Government information systems except national security systems and DoD information systems.
 - o Under an implementation plan signed by the President in August 2008, NSA is to provide DHS with the same technological capability that DoD uses to protect DoD systems. Because the capability involves classified information, it constitutes a national security system and NSA will provide technical assistance to DHS at its request.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

The Comprehensive National Cybersecurity Initiative (CNCI) also called the cyber initiative is directed in NSPD 54/HSPD 23 and the implementation plan. DHS is lead and it only covers federal government systems, not commercial. NSA is just providing technical assistance and services. Technical services typically refer to the decryption NSA will perform for DHS. NSA may not keep any of the data sent to NSA for decryption (with the exception of some crypto keys necessary for decryption services). NSA may not monitor .gov communications. If DHS is going to request technical assistance from NSA to look at .gov traffic, certain certifications and oversight must be done first. It may be that NSA could detail an analyst to DHS.

[1] P.L. 108-458, 118 Stat 3638, 17 December 2004.

(S) Global Defense of US Networks

- DHS or other federal agencies can use standard service provider authorities to monitor .gov networks for indications of malicious activity.
- Owners or operators of privately owned critical infrastructure systems can use service provider authorities to monitor their networks for indications of malicious activity but no federal agency has been provided general authority to perform such monitoring for privately owned networks.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

(S) Global Defense of US Networks

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123

- STRATCOM has been delegated CNA and CND-RA authority to attack foreign targets that threaten US interests .
- SECDEF in Nov 2009 placed Joint Task Force-Global Network Operations (JTF-GNO) under the operational control of Commander, CYBERCOM
- DIRNSA is now dual hatted as Commander CYBERCOM (May 2010).

SIGINT's role is not Defensive collection: SIGINT authorities allow NSA/CSS to monitor foreign systems for indications of foreign cyber attacks against US systems and disseminate that intelligence based on FI/CI/SMO requirements.

Classification:TOP SECRET//COMINT//Rel 4

EYES//20291123

- The officer serving as the Director, Defense Information Systems Agency (DISA) will continue to serve as Commander of JTF-GNO and will remain responsible for providing the JTF-GNO network and information assurance technical assistance as required.

(U) Additional Authorities

- DIRNSA is the Executive Secretary for all DoD, DoJ, and IC deconfliction regarding computer network attack and exploitation activities. (Trilateral DoD, DoJ, and IC MoA dated April 2007.)
- SECDEF designated the officer serving as DIRNSA to be the Commander, CYBERCOM (May 2010)
 - As directed by Commander, USSTRATCOM, CYBERCOM coordinates the development of, plans for, synchronizes, deconflicts, and executes cyber warfare to achieve global military objectives
 - JTF-GNO, OPCON to CYBERCOM, directs the operation and defense of the Global Information Grid

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

SCEs under NSA/CSS and JFCC-NW, esp in TAO ROC conduct CNE so those on the target networks day in and day out can be assigned to JFCC-NW for the time necessary to conduct the CNA activities. DIRNSA/CDR JFCC-NW issued memorandum allowing NSA/CSS personnel to be detailed to JFCC-NW for the time necessary to conduct the CNA, then they revert back to doing CNE. These personnel can conduct CNE while conducting CNA. Personnel detailed to JFCC-NW get training on the execute order, standing rules of engagement, and supplemental rules of engagement.

(S) Global Defense of US Networks

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123

- The Federal Information Security Management Act (FISMA) left intact the roles assigned to NIST and NSA but provides the Office of Management and Budget (OMB) an expanded information security oversight responsibilities over all Executive Branch departments and agencies. OMB required to set up a central Federal information security incident center which is US CERT.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

FISMA: 44 U.S.C. 3541 et seq., P.L. 107-347, 116 Stat 2899, 25 November 2002.

The Intelligence Reform and Terrorism Prevention Act of 2004[1] required the President to create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and civil liberties. The President was to designate a program manager responsible for information sharing across the Government who would issue standards, procedures, and guidelines for the operation of the information sharing system that are consistent with guidance from the President, OMB, and the DNI. Today, the program manager is in the Office of the DNI.

(S) Global Defense of US Networks

- FISMA cont. Agencies with national security systems are to share information about information security incidents, threats, and vulnerabilities with US CERT to the extent consistent with standards and guidelines for such systems issued in accordance with law and as directed by the President.
- The Homeland Security Act of 2002 gave the SECDHS wide access to information relating to threats of terrorism against the United States and to all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

(S) Implementing the PROCEDURES

1. You are targeting using a [REDACTED] signature in SIGINT. You see that the [REDACTED] put a trojan into the UMD web server. Can you query using the UMD web server IP address in Bluesash/Tutelage?
2. You see in Bluesash/Tutelage that the UMD mail server sent a trojan to the DoD NIPRNET. You believe it is a [REDACTED]. Can you task the UMD mail server IP address in SIGINT?

Classification: SECRET//COMINT//Rel 4
EYES//20291123

1. Yes, can look for anything suspicious in the IA data to protect the system. The initial SIGINT can be disseminated in a report if it satisfies a FI/CI/SMO requirement. If task the Bluesash/Tutelage deny list, must obtain dissemination approval.
2. No, not as a direct hit but may use a [REDACTED] signature in conjunction with the UMD mail server IP address.
3. The collection is valid. The target is a foreign person overseas. No USG communications because the target is not communicating with a legitimate USG official or employee or even a legitimate USP. All the exfiltrated data is incidental. Use dissemination procedures. Because this type of exfiltrated data potentially can contain so much USP information, OGC advises that this type of exfiltrated data be segregated from the rest of the SIGINT raw traffic and is made available only to those who have the mission to collect/report on these types of foreign intrusions. The exfiltrated data does not contain any FI other than what is reported in order to understand what the foreign hacker was seeking, and what the foreign hacker obtained for damage assessments.

(S) Implementing the PROCEDURES

You are targeting an [REDACTED] hacker has implanted a US company's computer overseas. You are collecting the [REDACTED] exfiltration of information and communications from that US company's computer that contains communications between the US company and a US Government organization.

Is the collection valid?

Do you have USG communications.

What do you do with the information?

Classification: SECRET//COMINT//Rel 4
EYES//20291123

1. Yes, can look for anything suspicious in the IA data to protect the system. The initial SIGINT can be disseminated in a report if it satisfies a FI/CI/SMO requirement. If task the Bluesash/Tutelage deny list, must obtain dissemination approval.
2. No, not as a direct hit but may use a [REDACTED] signature in conjunction with the UMD mail server IP address.
3. The collection is valid. The target is a foreign person overseas. No USG communications because the target is not communicating with a legitimate USG official or employee or even a legitimate USP. All the exfiltrated data is incidental. Use dissemination procedures. Because this type of exfiltrated data potentially can contain so much USP information, OGC advises that this type of exfiltrated data be segregated from the rest of the SIGINT raw traffic and is made available only to those who have the mission to collect/report on these types of foreign intrusions. The exfiltrated data does not contain any FI other than what is reported in order to understand what the foreign hacker was seeking, and what the foreign hacker obtained for damage assessments.

(U//FOUO) Reporting Conventions

- Need to know what data you are working with.
- Need to follow the correct purpose/procedures for the type of data collected. If reporting both SIGINT and IA information, must follow both rules.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

USSID 18 minimization is not sanitization. Policy governs sanitization to protect sources and methods. Important sometimes when have intrusion activity.

(U) Oversight & Compliance

- Oversight & Compliance is everyone's responsibility.
- Local management has responsibility to ensure day-to-day activities are carried out in accordance with applicable law and policy direction.
- SIGINT procedures must be followed for SIGINT collection, retention, and dissemination.
 - IAD procedures must be followed for IAD collection, retention and dissemination. Dissemination taking both sets of procedures into account can be done.
 - Contrary to popular belief, it is usually smarter to ask permission first rather than seek forgiveness later.
 - OGC has personnel on-call 24X7 to answer questions.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

Refer to USSID SP 0018 and IAD Oversight and Compliance policy, IAD Management Directive 20.

(U) Oversight & Compliance on the NTOC floor

- Personnel from other organizations sit on the NTOC floor. NTOC has signed MoUs with these organizations granting the personnel “dual-parent” authority.
- These personnel are working under NSA SIGINT and IA authorities (as well as their own “parent” authorities) and may see the raw traffic. No Dissemination of Raw traffic back to the organizations themselves, must follow dissemination rules.
- The sharable SIGINT raw traffic does *not* include raw data derived from FISA/PAA/FAA nor FBI FISA.
- Any FBI FISA disseminated must retain the FBI FISA caveat on all further disseminations.

Classification: SECRET//COMINT//Rel 4
EYES//20291123

The idea of the NTOC floor is to allow all the personnel on the floor to be able to collaborate, indicate what information is relevant to their organizations mission and facilitate dissemination. However, dissemination back to the organizations themselves is a dissemination and must follow the dissemination rules.

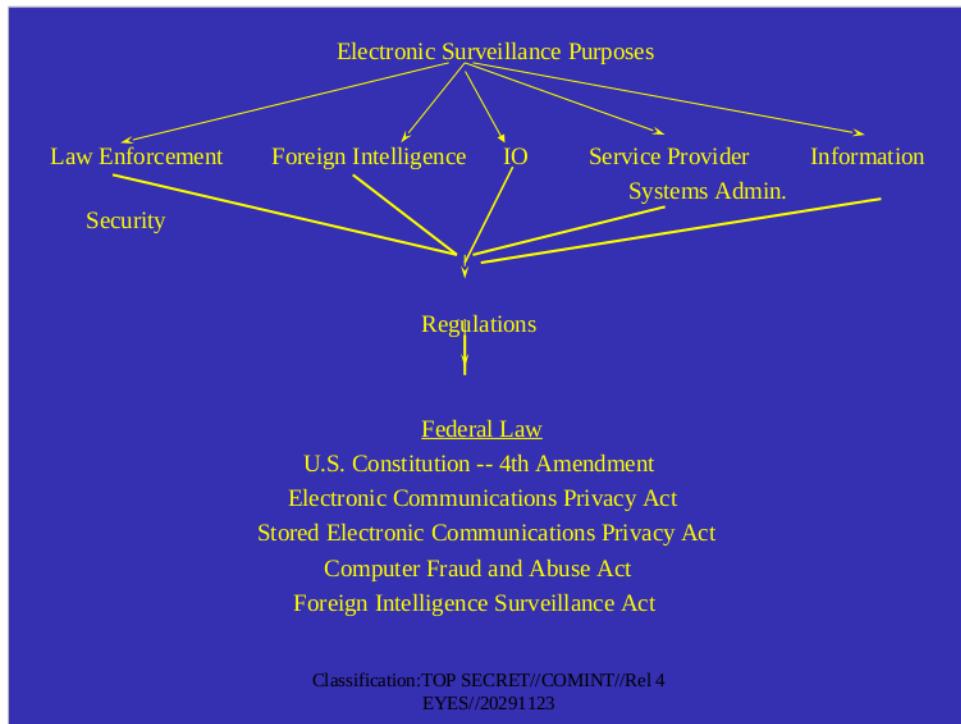
Questions to REMEMBER

- **What authorities are being used to collect information that I'm looking at?**
- **Where is this information being collected?**
 - SIGINT platforms? -Tutelage sensors? –Collateral source?
- **Who will receive access to the collected information?**
- **What retention and dissemination restrictions apply to the collected information**
 - (e.g., SIGINT Procedures, COMSEC Procedures, Service Provider Rules, etc.)?

Classification: UNCLASS//FOUO

?????? QUESTIONS ?????

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123



Many federal laws in this area because of information privacy rights.

Must follow the procedures that apply to the purpose. If mix purposes and procedures, may find themselves outside one of the exceptions to the federal laws.

[SECPA-diminished Expectation of Privacy but still need subpoena.]

CFAA-prohibits intentional, unauthorized access to a “protected computer” (I.e. any computer that has been or is involved in interstate commerce to include foreign computers) Exceed authorized access-protect from insider threat included. Allows intel and LE and protect activities. For protect, still need permission from the system owner.

COMSEC Monitoring

NTI SSD No. 600

- Telecommunications or information system's "owner" must request COMSEC services.
- Must certify existence of notification process that system's users know that their use of the system constitutes implied consent to COMSEC monitoring. CONSENT BANNERS
- Dissemination of collected information usually done without attribution to a particular individual.
 - 2 exceptions-passing of classified info.
 - Evidence of a significant crime or it is necessary in order to mitigate the vulnerability.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

Used really only by JCMA

Non attribution because purpose is to secure systems, not to be punitive.

(S) NSCID 6

- DIRNSA is tasked with establishing an effective, unified organization and controlling all SIGINT collection and processing activities of the United States so that it is effective, efficient, and coordinated.
- Toward this end, the Central Security Service (military SIGINT) was established under the DIRNSA, in accordance with a plan approved by the SECDEF.
- SIGINT includes Electronics Intelligence (ELINT) and Communications Intelligence (COMINT).
- COMINT is technical and intelligence information derived from foreign communications by other than the intended recipients.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

Mention something about ELINT not having an expectation of privacy but is still bound by the FI/CI/SMO mission of NSA.

(U) Authorities Continued

- Develop Computer Network Attack capabilities,
 - Not employ
- Conduct analysis of foreign information infrastructure systems for CNA technology development,
- Develop analytic modeling and simulation techniques to characterize vulnerabilities of information systems and effectiveness of developed CNA techniques.
- SecDef Memo dated 3 March 1997.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

Because NTOC works closely with JFCC-NW to provide support, provide info on other computer network related authorities at Ft Meade.

NSA's CNE and CNE enabling activities can easily be converted to CNA capabilities. NSA's purpose is to conduct or enable CNE. Sometimes fine line between CNE enabling and CNA. Look at purpose and what the capability does.

Funding can be an issue.

NSA does not have authority to conduct CNA

(S) NSCID 6, dated 17 February 1972

- DIRNSA responsible for the SIGINT mission of the United States, except for certain SIGINT activities conducted in support of clandestine CIA operations (NSCID 5)
- Pursuant to his SIGINT authority, DIRNSA has promulgated USSID SP0018 and other policies to govern the collection, processing, retention, and dissemination of SIGINT, especially SIGINT that includes US person information.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

(S) NSCID 6

- COMINT activities shall be construed to mean those activities that produce COMINT by the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means, and by the processing of foreign encrypted communications, however transmitted.
- Collection comprises search, intercept, and direction finding.
- Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results.

Classification:TOP SECRET//COMINT//Rel 4
EYES//20291123

I don't' go over this in any detail at all. The important piece is the definition and how the SCEs fit.

(U) Appendix D: Evaluation of the Comprehensive National Cybersecurity Initiative

(U) Presidential Directive NSPD-54/HSPD-23, *Cybersecurity Policy*, established “United States policy, strategy, guidelines, and implementation actions to secure cyberspace.” It includes a Comprehensive National Cybersecurity Initiative (CNCI), created to strengthen policies for protecting U.S. Government information and systems, clarify roles and responsibilities of Federal agencies related to cybersecurity, and explore how the Federal government might enhance its relationship with the private sector in order to better protect our critical infrastructures. The resourcing and implementation of the CNCI has been undertaken by the Federal government with a sense of urgency that reflects the nature and severity of the threat. The major “initiatives” within the CNCI are:

- Manage the Federal Enterprise Network as a single network enterprise, with Trusted Internet Connections that collapse the number of portals between government networks and the Internet;
- Deploy consistent intrusion detection capabilities across the Federal enterprise;
- Pursue deployment of intrusion prevention systems across the Federal enterprise;
- Catalogue, coordinate and redirect as appropriate cyber research and development efforts;
- Connect current cyber centers to enhance cyber situation awareness;
- Develop a government-wide cyber counterintelligence plan;
- Increase the security of classified networks;
- Expand cyber education;
- Define and develop enduring “leap-ahead” technology, strategies, and programs;
- Define and develop enduring deterrence strategies and programs;
- Develop a multi-pronged approach for global supply chain risk management; and
- Define the Federal role for extending cybersecurity into critical infrastructure domains by working with the private sector.

(U) These major portions of the CNCI required strengthening key strategic foundational capabilities within the Federal government, hence the CNCI includes several strategic “enablers” that augment ongoing cyber-related activities at specific departments and agencies:

- Ensuring adequate support to neutralize, mitigate, and disrupt domestic illegal computer activity;
- Increasing information assurance programs and activities;
- Increasing predictive, behavioral, information and trend analysis of foreign intrusion activities and computer network operational threats;
- Expanding and enhancing U.S. offensive capabilities in support of network defense;
- Increasing investment in U.S. Government cryptanalysis;
- Developing, deploying, and managing an intrusion response capability; and
- Monitoring and coordinating implementation of the CNCI.

(U) Significant CNCI accomplishments to date include rapid progress on many of the initiatives and their strategic enablers; extensive engagement with the Congress; the development of a consolidated view of the disparate budget resources committed to cyber programs funded under national intelligence, military, information assurance, law enforcement, and civilian agency program budgets; and the initiation of key out-of-cycle resource and acquisition activities that would have been difficult within normal legislative appropriations schedules. As a consolidated portfolio scarcely more than one year in existence, the results achieved have been overwhelmingly positive, and although challenges remain, the objectives are clear and in keeping with the larger strategy. The Federal government should continue to go forward with CNCI implementation.

(U) NSPD-54/HSPD-23 assigned responsibility for monitoring, coordinating, and reporting on implementation of the CNCI to the Director of National Intelligence (DNI), despite the fact that much of the CNCI portfolio falls outside of the Intelligence Community. The DNI has done a commendable and effective job using a Joint Interagency Cyber Task Force (JIACTF) created to carry out these responsibilities. The JIACTF uses a portfolio approach—complete with detailed performance measures and target achievement goals—for tracking the status of the 19 separate initiatives and enablers. Under this approach, the JIACTF serves as the central “steward” for oversight and monitoring, but unlike a traditional joint program management office, individual departments and agencies maintain responsibility for the development of business requirements, program management, and budgeting for each specific initiative and activity.

(U) As anticipated by individual CNCI component implementation plans, much work remains to achieve the objectives of the CNCI program and of NSPD-54/HSPD-23. Progress has been uneven, and subsequent oversight must put greater emphasis on scalability and sustainability. While the “steward” model for monitoring and coordinating CNCI activities has been effective as a start-up approach for a complex, multi-agency portfolio, stronger central coordination and oversight will be required to ensure that the individual components are commensurately resourced and mesh effectively to attain the required joint operating capabilities. Only the White House has sufficiently broad authority to provide the required central leadership. JIACTF-like staff support would be necessary to sustain and strengthen the interagency coordination that has been a hallmark of the CNCI successes. Anticipated outcomes

would include more effective collaboration and development of joint standard operating procedures where needed; more fully integrated program acquisition and management; and accelerated opportunities for technology training and re-use.

(U) The CNCI and associated activities identified by NSPD-54/HSPD-23 must evolve to become key base elements of the broader, updated national cyberspace strategy. Successful programs within NSPD-54/HSPD-23 should proceed apace; other programs are keys to the overall success of the strategy but have not fully matured or achieved their anticipated results. Where necessary, “Go Forward” recommendations should endorse the objectives of these programs and provide new direction for resolving roadblocks as well as considering innovative alternatives to accomplish the objectives.

(U) Status of CNCI Activities

(U) The JIACTF, in its “monitoring and coordinating” role, has highlighted areas of concern with CNCI implementation and recommended areas for course correction and has highlighted successes within the CNCI that could be expanded as the program advances. The 60-day cyberspace review team, based on inputs from the JIACTF, the Office of Management and Budget (OMB), and the departments and agencies, makes the following observations about the various CNCI components:

(U) Initiative #1. **Manage the Federal Enterprise Network as a single network enterprise, with Trusted Internet Connections (TICs).** Currently, Federal government networks have thousands of Internet access points that have proven to be too difficult to manage and secure. This Initiative, the primary purpose of which was publicly announced in November 2007,¹⁰⁶ aimed to cut the number of portals between government and the Internet to fewer than 100, using the General Services Administration award of the NETWORX contract for telecommunications service and the Federal Desktop Core Configuration (FDCC) to implement secure desktop configurations. *These program goals and timeframes have proven to be overly ambitious: the TIC and NETWORX consolidation initiative is behind schedule and unlikely to achieve its goal of delivering less than 100 connections either in short- or mid-term timeframes.*

(U) Initiative #2. **Deploy an intrusion detection system of sensors across the Federal enterprise.** Intrusion Detection requires software to identify when unauthorized entities have gained access to computer networks. The Department of Homeland Security (DHS) EINSTEIN 1 software package offers “after the fact” analysis of network flow information from participating Federal agencies and provides a high-level perspective from which to observe potential malicious activity in computer network traffic. The updated version, EINSTEIN 2, incorporates network intrusion detection technology capable of alerting the U.S. Computer Emergency Readiness Team (US-CERT) in real time to the presence of malicious or potentially harmful computer network activity in federal executive agencies’ network traffic based on specific pre-defined signatures derived from known malicious activity. DHS reviewed the legal and privacy implications of this system and published a Privacy Impact Assessment for EINSTEIN 2 on its website,¹⁰⁷ thereby providing greater transparency for this part of the CNCI than for most of the other program elements. *Unfortunately, EINSTEIN 2 was envisioned for deployment at the Trusted Internet Connections established by Initiative #1—and hence this Initiative’s deployment schedule has slipped because of the slippage in the TIC and NETWORX consolidation.*

¹⁰⁶ (U) <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf>

¹⁰⁷ (U) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

(S//REL TO FVEY) Initiative #3. **Pursue deployment of intrusion prevention systems across the Federal enterprise.** Intrusion prevention requires a capability to not only identify intrusions in progress, but to block the attacker from successfully entering the network. Work is under way on developing EINSTEIN 3, a sensor-based system that will automatically block or otherwise mitigate the impact of attempted cyber intrusions. In practice, intrusion prevention is a capability required and routinely deployed by private industry, typically through managed security services offered by Internet Service Providers and Data Exchange Internet Exchange Points, and for home users through commercially available firewall and antivirus programs. The Initiative #3 plan offers advantages unavailable commercially, in particular NSA cryptanalysis and decryption services to address threats masked by encryption. The linkage of EINSTEIN 3 to the NSA Signals Intelligence system, similar to the system already being deployed to defend Department of Defense networks, raises civil liberties and privacy concerns that have significantly complicated EINSTEIN 3 development. *The need for sophisticated intrusion prevention capabilities for government networks is beyond question. There also is a need for greater transparency and public dialogue on the means by which this will be accomplished, taking into account civil liberties and privacy concerns while remaining mindful of the need to protect from release any information that would allow adversaries to subvert U.S. defenses. Given the significant challenges facing this implementation as well as those of Initiatives #1 and #2, EINSTEIN 3 implementation should proceed with a) enhanced transparency and dialogue to address civil liberties and privacy concerns, and b) concurrent assessment of additional implementation concepts that could reduce risks to program implementation while meeting the goals and objectives of Initiative #3.*

(U) Initiative #4: **Coordinate and redirect research and development efforts.** No single individual or organization is aware of all of the cyber-related R&D activities being funded by the Federal government. This Initiative remains critical to determining whether there is redundancy, figuring out research gaps, and ensuring the taxpayers are getting full value for their money as we shape our strategic investments. *Our review determined that a successful process has been created, and the government is beginning to identify shortfalls needing additional investment and those where overlap exists.*

(U) Initiative #5: **Connect current cyber centers to enhance situation awareness.** There is a pressing need to ensure that government information security offices and cyber operations centers share data as legally appropriate regarding malicious activities against federal systems in order to have a better understanding of the entire threat to government systems. This effort focuses on key aspects necessary to enable practical mission bridging across the elements of U.S. cyber activities: network connectivity, common information standards, and shared standard operating procedures. *The review determined that full connectivity at all levels of data classification does not yet exist between the centers, and the continued use of disparate toolsets complicates the development of common situation awareness. The success of this Initiative requires reconsideration of its governance structure and its resourcing requirements.*

(U) Initiative #6: **Develop a government-wide cyber counterintelligence (CI) plan,** encompassing development of a plan across agencies to identify, analyze, share information, and respond as appropriate to foreign-sponsored cyber intelligence threats to the United States. This government-wide Cyber CI Program plan is aligned with the *National Counterintelligence Strategy of the United States of America*—which predates the creation of the CNCI—and supports the other programmatic elements of the CNCI. *The plan is in place and execution is under way, although out-year funding remains a concern.*

(U) Initiative #7: **Increase the security of our classified networks.** These are the networks that house the Federal government's classified and most sensitive information. *A detailed implementation plan has been approved for some Federal government components, although issues surrounding the authorities needed to enforce the plan remain unresolved, as do funding concerns associated with government-wide implementation.*

(U) Initiative #8: **Expand cyber education.** There are too few cybersecurity experts within the Federal government or private sector to adequately implement the CNCI, nor is there an adequately established Federal cybersecurity career field to build upon. Cyber training and personnel development programs, while good, are limited in focus and lack unity of effort. In order effectively to address the scope of the cyber threat, we must develop a technologically-skilled and cyber-savvy workforce and ensure an adequate pipeline for the future. *Our review concluded that the current effort is behind schedule, lacks focus, and requires additional senior level policy guidance.*

(U) Initiative #9: **Define and develop enduring “leap-ahead” technology, strategies, and programs.** One goal of the CNCI is to develop technologies that provide increases in cyber security by orders of magnitude above our current systems and which are deployable 5 to 10 years hence. The Federal government has begun to outline Grand Challenges for the research community to help solve these hard problems, which require “out of the box” thinking. In dealing with the private sector, the government is identifying and communicating common needs that should drive mutual investment in key research areas. In this regard, the government has publicly issued three Requests for Input.¹⁰⁸ *An approved plan is in place and is proceeding well, although some elements are behind schedule in implementation.*

(U) Initiative #10: **Define and develop enduring deterrence strategies and programs.** Senior U.S. policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem, and these measures have not achieved the level of security needed. *This Initiative is proceeding methodically to build an approach to cyber defense strategy that deters interference and attack in cyberspace using such tools as warning and communication of “red lines”, roles for private sector and international partners, and appropriate response by both state and non-state actors. Outreach to a number of key constituencies that can contribute to the development of this strategy has been successful. Out-year funding remains a concern and implementation of the previously approved strategy is lagging.*

(U) Initiative #11: **Develop a multi-pronged approach for global supply chain risk management.** Today's information technology marketplace often provides insufficient software assurance, hardware assurance, or data integrity assurance. Risks stemming both from the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. *Managing this risk requires greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; development and employment of tools and resources to mitigate risk technically and operationally across the lifecycle of products (from design*

¹⁰⁸ (U) As stated on the website of the Networking and Information Technology Research and Development (NITRD) Program, “[O]ver 160 responses were submitted to the first RFI issued by the NITRD SSG (October 14, 2008), indicating a strong desire by the technical community to participate. RFI-2 (issued on December 30, 2008) expanded the opportunity for participation by permitting submitters to designate parts of submissions as proprietary. RFI-3 presents prospective cyber security categories derived from responses to RFI- 1 for further consideration.” http://www.nitrd.gov/leapyear/NCLY_RFI-3.pdf

through retirement); and development of new acquisition policies and practices that influence industry to develop and adopt supply chain and risk management standards and best practices. One significant Federal component—the Department of Defense—has issued policy guidance assigning roles and responsibilities and is proceeding to pilot implementation of its approach. This Initiative must continue with increased emphasis on expanding education about supply chain risks and on including more government and private sector communities.

(U) Initiative #12. **Define the Federal role for extending cybersecurity into critical infrastructure domains.** Dialogue about cyber security between the Federal government and the private sector (which owns and operates most of the U.S. critical cyber infrastructure) is essential and has been ongoing for well over a decade. It is widely accepted that the government needs to gain and share with the private sector an operational understanding of how adversaries create and exploit our cyber vulnerabilities, including an assessment of the extent and reach of these adversarial activities and informing the private sector of what is being targeted and, if possible, why. *Progress is being made on multiple fronts, but the government's efforts are not well aligned and, as a result, create an undue burden on private-sector entities that wish to work with the government but cannot commit the resources necessary to participate in multiple forums. As a result, this Initiative should proceed while cataloguing current efforts, determining overlaps and gaps, and communicating in a more streamlined manner with industry.*

(S//REL TO FVEY) Strategic Enablers:

- **Ensure adequate support to neutralize, mitigate, and disrupt domestic illegal computer activity.** *This law enforcement-led activity has made significant operational progress, especially with respect to the establishment and implementation of the FBI's National Cyber Investigative Joint Task Force.*
- **Increase Information Assurance programs and activities:** *This activity is making progress and is poised to serve as a model for wider Federal adoption.*
- **Increase predictive, behavioral, information and trend analysis of foreign intrusion activities and computer network operational threats:** *Foundational work to build the requisite workforce and analytic framework is under way consistent with the strategic plan.*
- **Increase investment in U.S Government cryptanalysis:** *Capabilities are under development.*
- **Develop, deploy, and manage an intrusion response capability:** *Substantial research and development is under way, and capabilities are being field tested within the Department of Defense's .mil environment.*
- **Monitor and coordinate implementation of the CNCI:** *The Joint Interagency Cyber Task Force model of a "steward" coordinating implementation has worked for the CNCI's start-up operations, but is not scalable or sustainable over the entire life-cycle of the program. It should evolve to a stronger central White House leadership effort.*

(U) The following table provides an overview of the status of the CNCI programs along with major recommended actions. The strategic goals of each of the CNCI programs are sound. An evaluation of

“Green” reflects that the strategy is sound and its implementation is proceeding as expected; “Yellow” indicates that progress is lagging and requires attention but that successful implementation of the strategy is still expected; “Orange” indicates that alternative strategies should be considered but work should continue in the meantime; “Red” indicates that implementation is so far off course that an alternative strategy is required.

This table is S//REL TO FVEY

CNCI Initiatives	Recommendation	Evaluation
Initiative 1: Trusted Internet Connections	<ul style="list-style-type: none"> • Review and re-baseline implementation schedule and approach • Subsequent strategy must incorporate all connection types (SATCOM, Wi-Fi, Cable) • Reconcile implementation timeframes with other Federal legislation (stimulus investments, omnibus budget provisions) • Evaluate alternatives for achieving compliance with security objectives 	Orange
Initiative 2: Deploy Passive Sensors Across Federal Systems	<ul style="list-style-type: none"> • In light of Initiative 1 delays, continue Einstein 2 while evaluating complementary approaches to achieve Initiative 2 goals • Engage Congress and private sector interests in public dialogue regarding intrusion detection approaches and U.S. Government requirements 	Orange
Initiative 3: Deployment of Intrusion Prevention Systems	<ul style="list-style-type: none"> • Engage Congress and private sector interests in public dialogue regarding intrusion prevention approaches and U.S. Government requirements • Work with the Attorney General, OMB, White House, and the Office of the DNI to fulfill legal, civil liberties, and privacy requirements already described in implementation plans • Assess additional implementation concepts that could reduce risks to program implementation while meeting the goals and objectives of Initiative #3 	Yellow
Initiative 4: Coordinate and Redirect Research and Development Efforts	<ul style="list-style-type: none"> • Continue as planned 	Green

This table is S//REL TO FVEY

CNCI Initiatives	Recommendation	Evaluation
Initiative 5: Connect Current Cyber Centers To Enhance Situational Awareness	<ul style="list-style-type: none"> Identify resources to proceed with connectivity or for collocation of centers Develop integrated program/budget/ governance strategy for ensuring that individual tool capabilities may be acquired and used by all participants Establish data and product standards and an operational framework for common situation awareness and reporting 	Yellow
Initiative 6: Develop a Government-Wide Cyber Counter-intelligence Plan	<ul style="list-style-type: none"> Evaluate as objectives are reached Need to ensure agencies are programming funds for next program build in order to pay for activities 	Green
Initiative 7: Secure Classified Networks	<ul style="list-style-type: none"> Evaluate as milestones reached Need to ensure agencies are programming funds for next program build in order to pay for activities 	Green
Initiative 8: Expand Cyber Education	<ul style="list-style-type: none"> Completely reshape to include a strategy for national-level leadership, comprehensive training programs, and broad-based public dialogue 	Red
Initiative 9: Define and Develop Enduring Leap-Ahead Technology, Strategies, and Programs	<ul style="list-style-type: none"> Need to accelerate program activities 	Yellow
Initiative 10: Define and Develop Enduring Deterrence Strategies and Programs	<ul style="list-style-type: none"> Need to implement key recommendations from previously approved strategy 	Yellow
Initiative 11: Develop Multi-Pronged Approach for Global Supply Chain Risk Management	<ul style="list-style-type: none"> Continue to identify pilot programs Determine resource requirements for threat evaluation support to all departments and agencies Evaluate existing legal framework for effecting rapid, threat-based procurement 	Yellow
Initiative 12: Define the Federal Role for Extending Cybersecurity into Critical Infrastructure	<ul style="list-style-type: none"> Accelerate review of policy, legal, process, and resource barriers Ensure agencies are programming funds for next program build Catalogue, distinguish, and align current public/private partnerships 	Yellow

This table is S//REL TO FVEY

CNCI Enablers		
<i>Ensure Adequate Support To Neutralize, Mitigate, and Disrupt Domestic Illegal Computer Activity</i>	<ul style="list-style-type: none"> Consider how to expand capacity between and among federal, state and local law enforcement entities 	Green
<i>Increase DoD Information Assurance</i>	<ul style="list-style-type: none"> Evaluate mechanisms for deploying capabilities more quickly Increase cybersecurity policy training efforts 	Green
<i>Strategic Analysis of Intrusion Activities and CNO Threats</i>	<ul style="list-style-type: none"> Evaluate how this analytic effort will dovetail with other departments and agencies 	Yellow
<i>Increase Investment in U.S Government Cryptanalysis</i>	<ul style="list-style-type: none"> Continue long-term investment Evaluate additional national cybersecurity needs 	Green
<i>Develop, Deploy, and Manage an Intrusion Response Capability</i>	<ul style="list-style-type: none"> Continue to evaluate solution Resolve issues associated with adaptability for extending to state, local and private sectors 	Yellow
<i>Monitor and coordinate CNCI</i>	<ul style="list-style-type: none"> Identify single National Cyber Mission Owner Reaffirm CNCI roles and responsibilities to maintain momentum 	Green

SECRET//REL TO FVEY

CYBERSPACE POLICY REVIEW

(U) Appendix E: Case for Developing an International Cybersecurity Policy Framework

(U//FOUO) The United States lacks a comprehensive strategic international policy framework and coordinated engagement strategy that spans the full range of U.S. economic, national security, public safety and privacy interests in cyberspace. Before the United States can effectively engage its foreign partners, the U.S. Government first needs to make national-level decisions to:

- Identify and prioritize U.S. national interests in cyberspace;
- Review existing U.S. Government policy positions regarding cybersecurity;
- Consider the strategic connections and possible contradictions between the numerous U.S. Government policy objectives for cybersecurity;
- Develop new or refined positions regarding cybersecurity (where needed);
- Effectively engage the private sector, since it comprises the owners and operators of a majority of the information and communications infrastructure;
- Prioritize multi-lateral forums, coordinate positions in them with our close allies and other foreign partners, and assess the appropriate U.S. Government representation for those events;
- Prioritize countries that pose the greatest challenges or opportunities for bi-lateral engagement on cybersecurity issues; and
- Move forward with coordinated diplomacy and outreach efforts across the executive branch, including more proactive and targeted engagement to advance agreed upon U.S. positions.

(U//FOUO) Based on the feedback that departments and agencies provided to the 60-day cyberspace policy review team and discussions with key allies and members of the private sector, the priority topics for international engagement can be conceptually organized into three broad categories: Internet governance, international law and security, and multi-lateral public policy. Recognizing that several of the issues identified within these categories have implications extending beyond cybersecurity and require broader coordination, they all have a significant international component involving cybersecurity that requires attention. All three categories should be addressed in a coordinated fashion to advance national objectives of global prosperity and security.

- First, Internet governance refers to the decision making process for developing secure architectures, technical standards, administrative procedures, and best practices at the international level and ensure the secure, resilient and operation of the Internet.
- Second, because cyberspace now constitutes the primary domain for global communications and commerce, it has become a critical national asset for many nations. This criticality may lead to reexamination of traditional questions of public international law and military doctrine (e.g., strategic deterrence) in this new context.
- Third, because of the global nature of communications networks, an array of public policy, regulatory, and law enforcement issues that are being addressed within independent domestic jurisdictions have wider ramifications for the United States and other countries. Domestic

policies developed in isolation could significantly hamper necessary interoperability and cooperation at both the regional and international levels. Better coordination is required so that competing policy interests (e.g., data privacy, security, commercial innovation, etc.) are balanced by individual countries in ways that account for the global effects of those policies.

(U//FOUO) Each of those three general areas, in turn, encompasses both substantive issues for determination and procedural considerations for international engagement. Not only should the U.S. Government reach its own policy decisions on specific issues after concerted discussion within the U.S. Government and with our allies, but it should also strategize how best to engage the rest of the world to support these positions. Key to that process will be public-private exchanges within the United States as well as careful selection of the multi-lateral forums that are best suited to considering, deciding, and advancing each aspect of international cybersecurity policy. The United States and its allies should select forums for affirmative policy advancement and recognize where it is necessary to participate in others for defensive reasons. The multiplicity of international organizations currently striving to set international policy in cyberspace, with some developing as independent proponents of policy, is taxing many countries' abilities to staff participation in those organizations and track their respective activities. This situation poses the risk of producing disjointed, conflicting, or incomplete solutions while allowing some countries to advance interests adverse to the United States or its allies in forums where engagement by the United States is insufficient.

(U) Internet Governance, Technical Oversight, and Standards Issues

(U//FOUO) One of the U.S. Government's highest priorities should be to determine, in concert with its close allies and other partners in the international community of Internet users, how to ensure the continued stability and global interoperability of the Internet, while increasing security and reliability for all users. A core component of this endeavor is how to ensure the secure and efficient operation of the domain name and addressing system (DNS).

(U//FOUO) Enhancing the security of the global Internet will require the identification, development, and deployment of new technical architectures; improved engineering standards and protocols; and possibly the adoption of revised best practices. Immediate issues in this area include assessment of the strategic options for deployment of the DNS security extensions protocol (DNSSEC) in the root zone, for encouraging its deployment throughout the Internet infrastructure, and for facilitating the smooth migration to Internet Protocol version 6 (IPv6). Other areas warranting attention include (but are not limited to) research and development of new methods and capabilities for identity management and authentication for certain types of online activity. Currently, these technical issues are being discussed in a range of specialized organizations like the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the International Telecommunication Union (ITU). As information and communications technologies continue to evolve, standards bodies will need to be able to adapt, identify, and promulgate new best practices and needed technical standards to address emerging needs of the next-generation architecture. The United States and its foreign partners should develop an action plan for working in these various forums to advance agreed upon strategic objectives in the standards area.

(U//FOUO) Finally, apart from the foregoing technical and operational matters, a broad range of other multi-lateral public policy issues also emanate from the operation of the Internet. These issues, some of which are more generally discussed below, hold strategic implications for the United States and its allies and cannot be fully or comprehensively addressed in any individual forum. They are presently the

subject of action in a range of organizations including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), the ITU, and other broader, multi-lateral venues such as the United Nations (UN), the G-8, the Organization for Economic Cooperation and Development (OECD), the Organization for Security and Cooperation in Europe (OSCE), and the Organization of American States (OAS). While recognizing that the international dialogue on these various issues should (and invariably will) continue in multiple forums, the United States and its foreign partners should assess for each strategic objective which forums are most advantageous for achieving desired outcomes.

(U) International Law and Security

(S//REL TO FVEY) The international community has not yet achieved consensus on several key concepts of international law as they pertain to cyberspace. Different countries apply the traditional legal notions of territorial jurisdiction, use of force, and humanitarian law inconsistently in the cyberspace context. Accordingly, the United States needs to consider how to establish collective, acceptable international norms and redlines for nation-state conduct in cyberspace. Before engaging in that dialogue, the U.S. Government should first balance the need for increased international cybersecurity with its own need to develop and employ cyber capabilities to protect U.S. national security. Given the growing dependence of all sectors of our society on the Internet, the United States also needs to recognize that the international scale of cybercrime, because of the growing severity of its cumulative effects, increasingly constitutes a national security concern in its own right.

(S//REL TO FVEY) Several international efforts are under way to define and address evolving concepts of cyber arms control, cyberterrorism, and cybercrime. For example, the Russian Federation has advanced the position in the UN, OSCE, and a plethora of other forums that a new arms control regime is required for cyberspace. The United States does not concur with the Russian position or a related argument they make that a new international instrument is required to deal with cyberterrorism (where that term is used to describe terrorist attacks on information systems). The United States' position has been that no new international agreements are needed in these areas and that work should instead focus on implementing strong cybersecurity and cybercrime provisions. With respect to cybercrime laws, the United States advocates the Council of Europe's Convention on Cybercrime as a way of building a common substantive and procedural criminal legal framework in countries around the world. Although the U.S. has worked with other countries on terrorist use of the Internet, that topic presents a number of challenges including differing legal protections for content and differing views on tactics and information sharing. The U.S. Government should take an active role in shaping international norms through its own diplomatic efforts, capacity building and military practices. The United States will need to determine its own national interests regarding a range of issues in cyberspace, carefully select the preferred forums for international policy development, and devise both affirmative and defensive issue positions that will enlist the support of other countries.

(S//REL TO FVEY) In addition, the United States and our allies will need to develop new technical capabilities, doctrines, and rules of engagement premised on any substantive future cybersecurity norms that are recognized by the international community. In the absence of effective technical methods for the timely attribution of cyber incidents, reliance on legal authorities that make theoretical distinctions between armed attacks, terrorism, and criminal activity may prove impractical. Moreover, what constitutes a proportional response in cyberspace is complicated by the fact that both public and private networks may be affected by a cyber action. Consideration should also be given to diplomatic and sovereignty issues where the networks of friendly countries are affected by a response. Another

key implementation priority is strategic deterrence. The United States should decide how state and non-state actors can be deterred, taking into account the general lack of credible verification procedures and reliable attribution methods.

(U) Multi-Lateral Public Policy

(U//FOUO) The global nature of cyberspace requires unprecedented cooperation to foster commercial interoperability, protect critical infrastructures, and enable effective transnational law enforcement. Cooperation and some consistent capability is required, in part, due to a “weakest link” problem; because malicious actors can easily route electronic attacks through the country with weakest domestic law, capacity or political will, every country needs robust, and relatively consistent, capabilities. The current discrepancies in national (or regional) data protection laws, substantive and procedural domestic criminal statutes, forensic capabilities, and investigative capacity all pose obstacles to international cooperation. By establishing consistent norms for non-state actors in cyberspace, ensuring that there is sufficient capacity and prioritization, and building and strengthening transnational cooperative networks for law enforcement and network defense, the international community could improve global critical infrastructure protection and law enforcement. Consideration of civil liberties, privacy rights, and other human rights, coupled with the recognition that good cybersecurity and law enforcement should enhance privacy, will be an integral part of this effort.

(U//FOUO) Accordingly, the United States, working with its allies, should continue to promote domestic legal structures, cooperative mechanisms, and national best practices in countries around the world. The United States will also need to prioritize resources (i.e., time, money, and personnel) and leverage the resources of its allies to build capacity through legislative, investigative, technical and other training of foreign partners. Moreover, in order to implement any mutually agreed policies, the United States will need to support greater information sharing both with other governments and the private sector (especially of time-sensitive and classified information, as necessary). Better information sharing will require identification of the best channels to use to share information, determination of the parties with whom it should be shared, and consideration of how information can be shared with multi-national companies.

(U//FOUO) Many of these substantive issues are already being discussed by international organizations, including the G-8, COE, EU, OSCE, and OECD. Implementation measures are also being pursued bilaterally with close allies, through U.S.-led regional programs, and through international organizations, such as the UN, the International Telecommunications Union, the North Atlantic Treaty Organization (NATO), the OAS, and the Asia Pacific Economic Cooperation (APEC) forum. Once again, the selection of preferred forums for international engagement on each relevant cybersecurity policy topic, and the prioritization of those topics, will eliminate redundancy, focus debate, and achieve more effective solutions.

(U//FOUO) The United States should also recognize and develop a strategy to address the domestic actions of countries that have a profound effect on U.S. businesses and security. As storage of computer data moves to “the cloud,” countries are increasingly requiring the data of its respective citizens be stored within its borders. Although the United States has occasionally required this as a condition of approving changes of ownership, it has no comprehensive policy on this issue. Some countries increasingly have demanded data from U.S. providers through subsidiaries of those companies located or operating within the foreign territory, even when access to that data, stored in the United States requires more stringent legal procedures under U.S. law. In addition, countries also have demanded

access to the source code of companies' software products as a condition of doing business in their jurisdictions. Censorship and free speech concerns are implicated when countries have laws restricting certain kinds of speech protected in the United States and try to apply that law to U.S. providers. Promotion of free speech is an even greater concern when authoritarian regimes seek to censor speech and put pressure on U.S. providers and subsidiaries to that end.

SECRET//REL TO FVEY

CYBERSPACE POLICY REVIEW

SECRET//REL TO FVEY