(U//FOUO) CNO LEGAL AUTHORITIES



Office of General Counsel

[redacted]

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

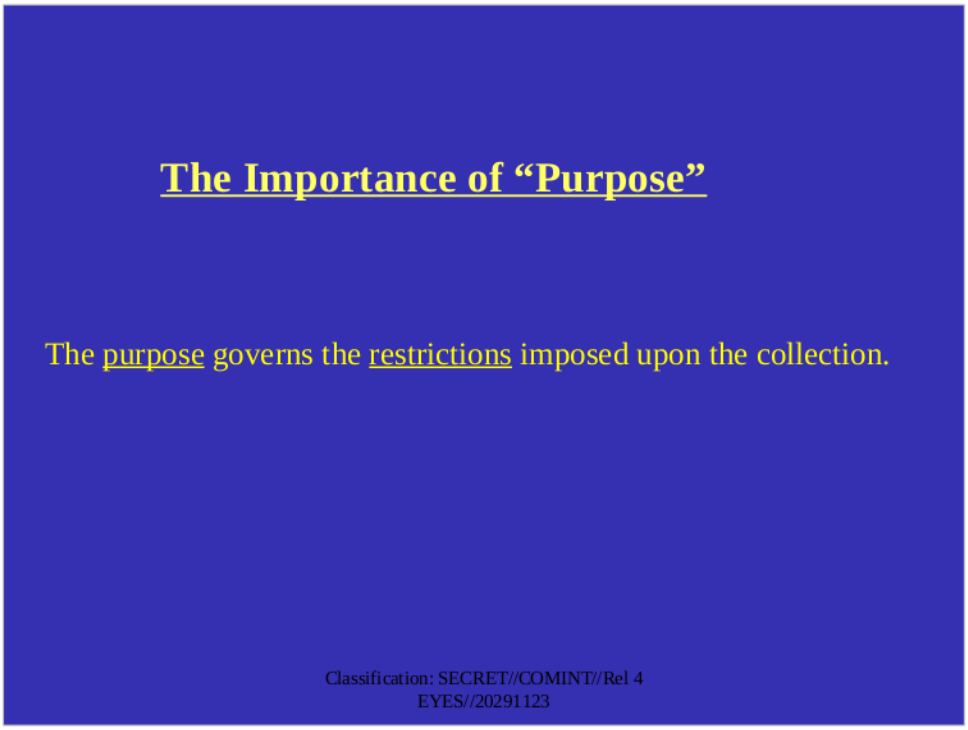
Objectives for Today's Brief

- Overview of SIGINT law
- Overview of Information Assurance Law

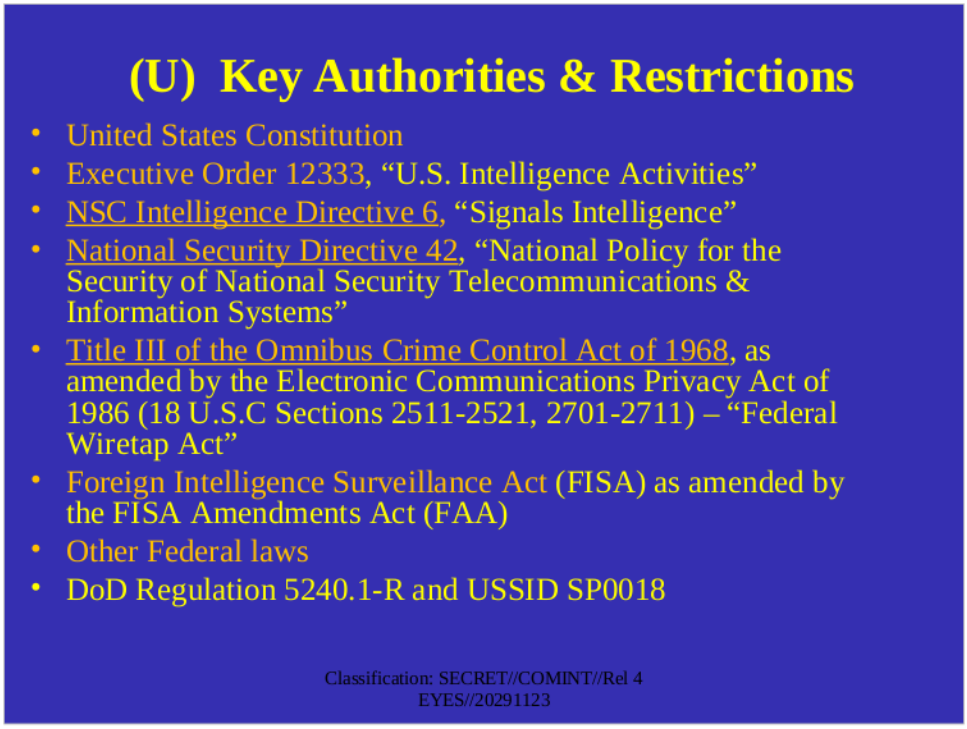
- What do I need to know?
- How do I apply this Stuff to what I'm doing?

(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.*)?**



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.



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
E.O. 13526, 20291123

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.

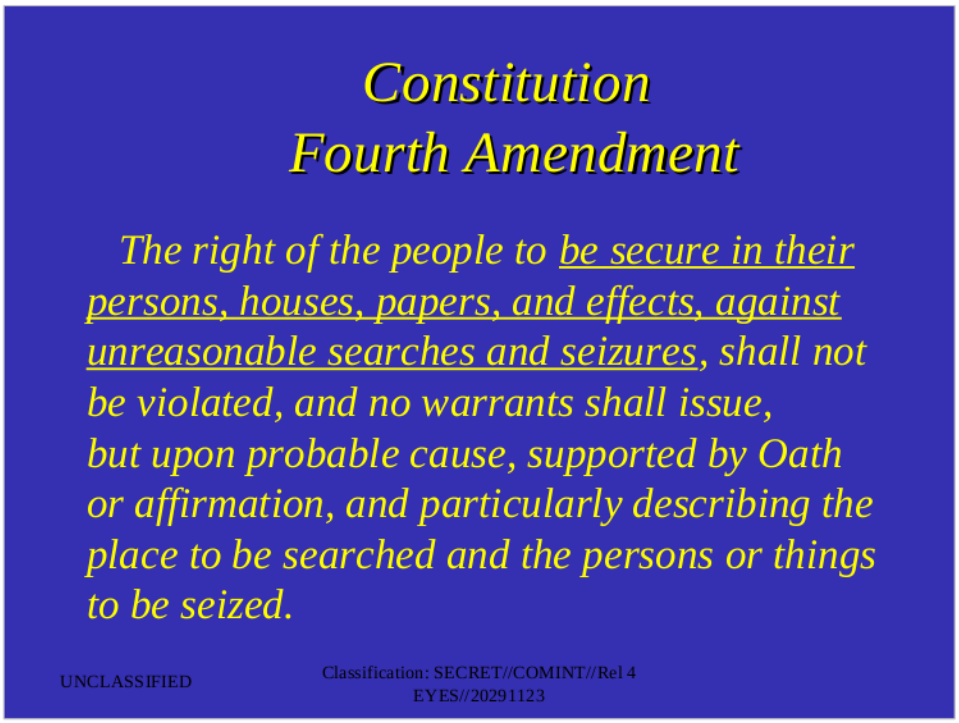
Authority to conduct CNE

- (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.



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...

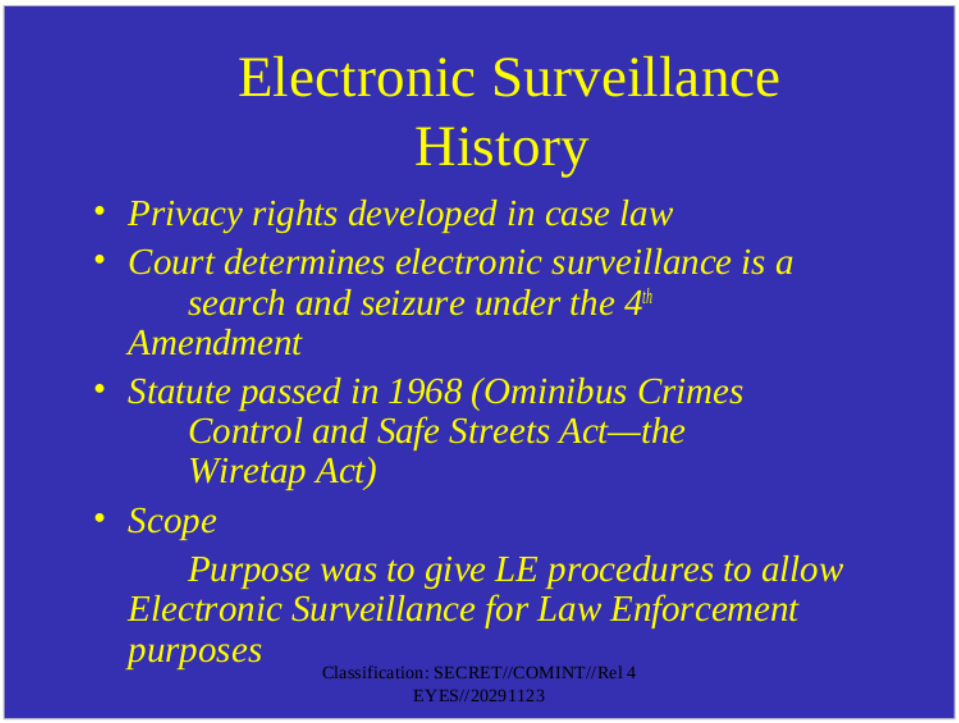
How it's done.

Where it's done.

Against whom it's done.

Why it's done.

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



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.



-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.



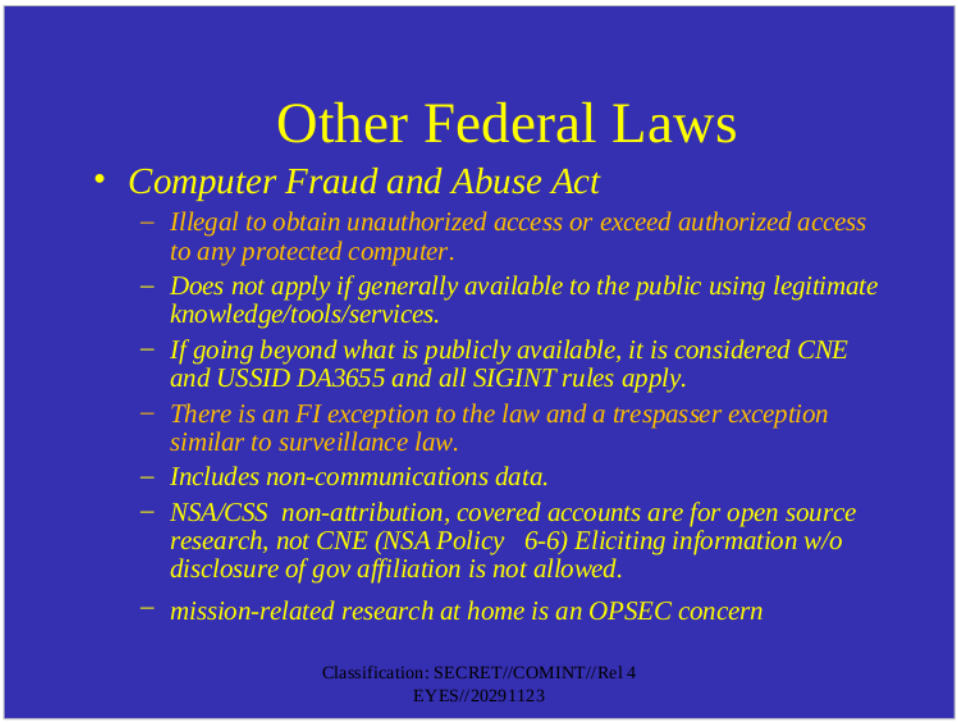
-Will talk about the FI exception when briefing SIGINT rules

-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.



-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.

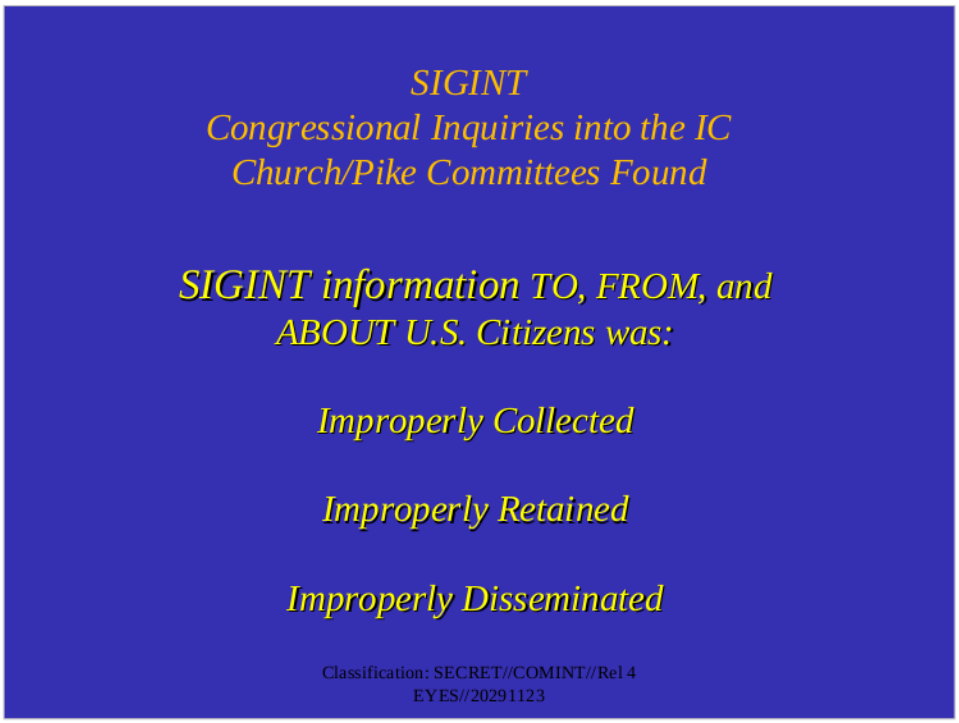
-NSA was granted authority from the President to collect not only COMINT but any other data at rest on a foreign target computer while conducting out CNE missions. (Also have a delegation from SECDEF for room audio and video.)

-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.



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.



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



FISA only applies to the FI/SIGINT collection.

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



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



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)*

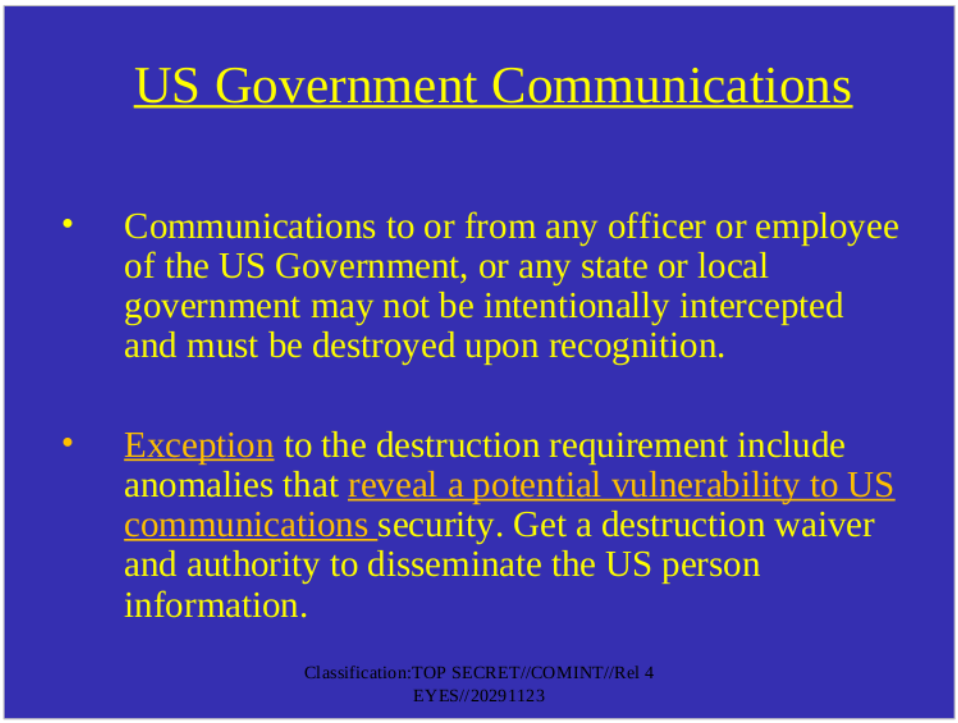
Classification: SECRET//COMINT//Rel 4 EYES//20291123

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

-If used a presumption, and you find out you have been targeting/collecting/disseminating communcations 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.



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.



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.

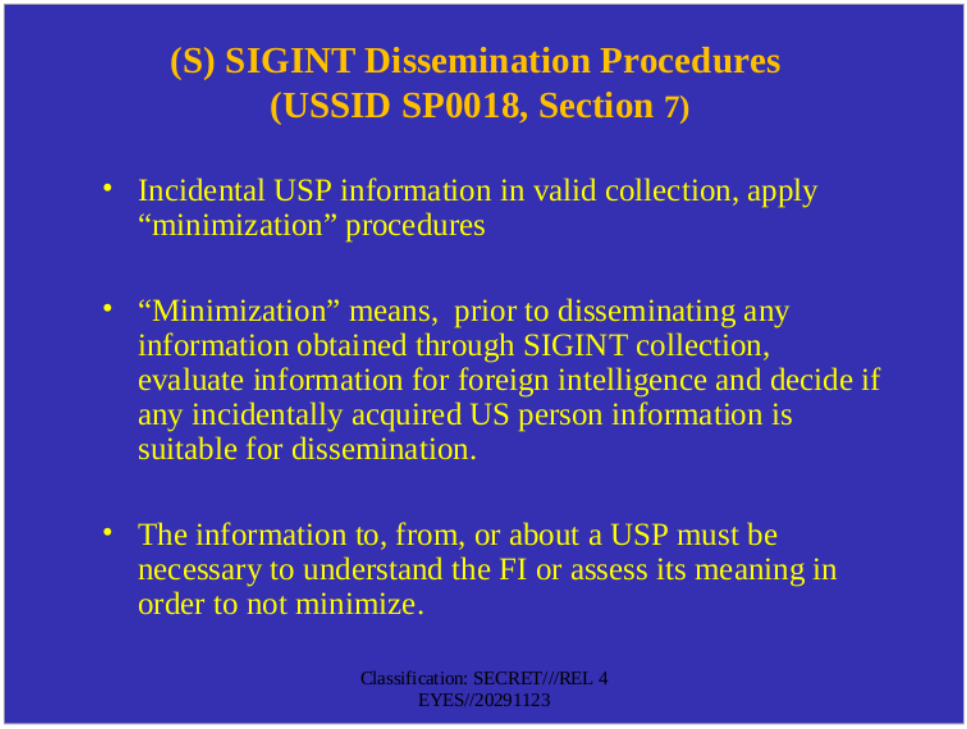
Targeting by Subject Matter
USSID SP0018, Section 5

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



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



-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.

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 EYES//20291123
UNCLASSIFIED//FOR OFFICIAL USE ONLY

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/abbettor, 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/abbettor/conspirator.



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

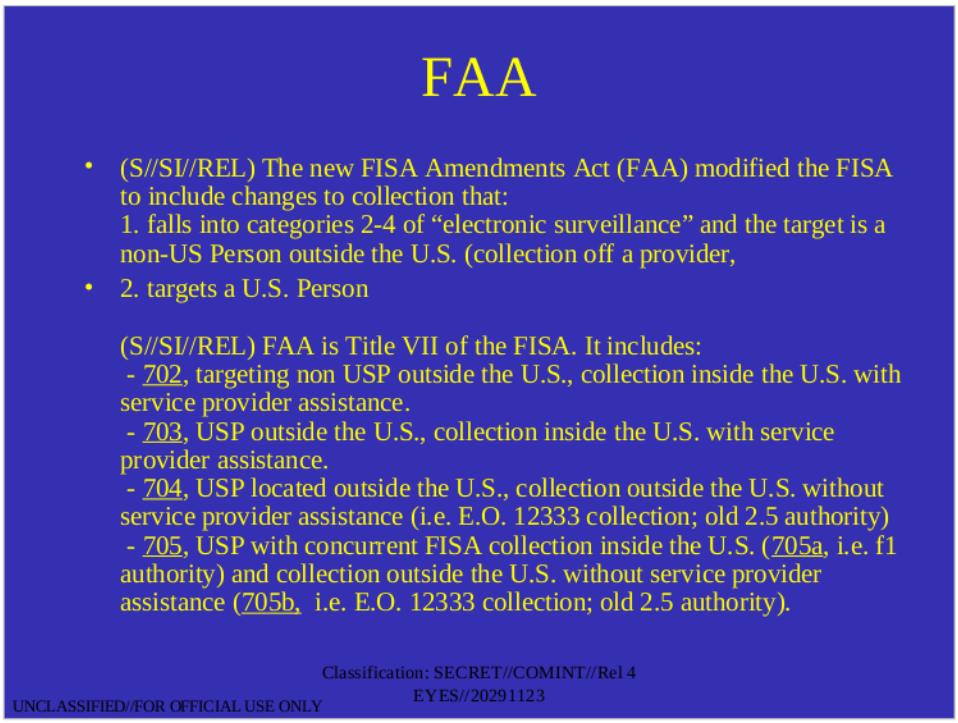
F4 is where CNE usually falls. Other devices includes accessing/CNE against a computer located in the U.S.

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.



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

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

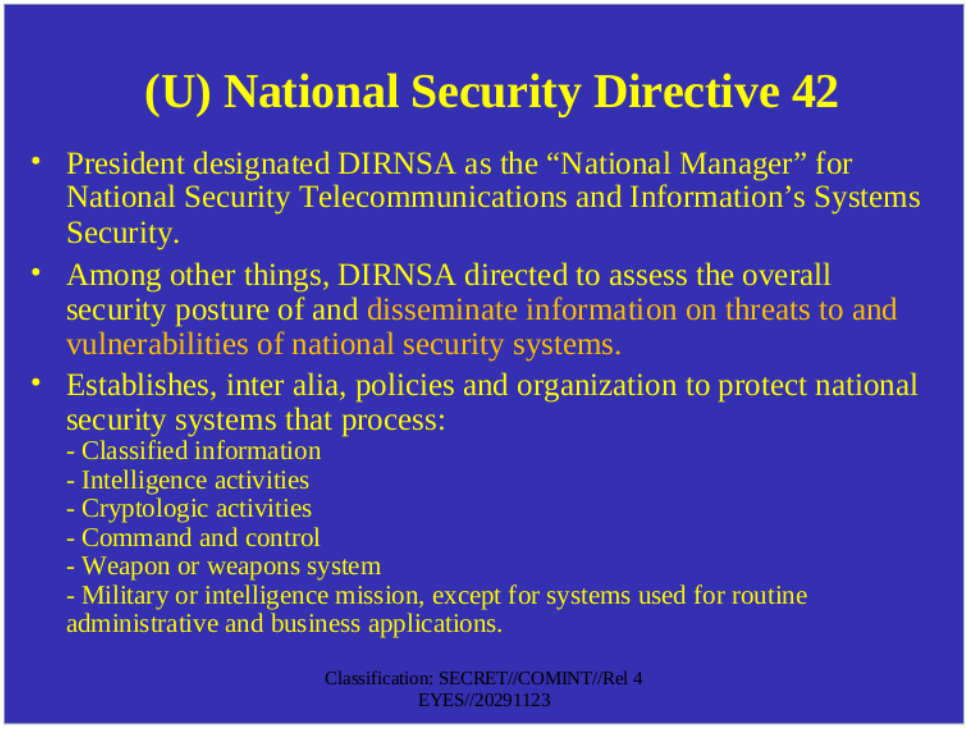


1. Request to select based on a foreign hacker signature in conjunction with a DoD military IP address. Nothing seen in SIGINT. The SIGINT system doesn't see everything. Collection architecture has to be in place. So, without asking, analyst put the DoD military IP address in as a straight hit and obtained 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.) My 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



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 to 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)

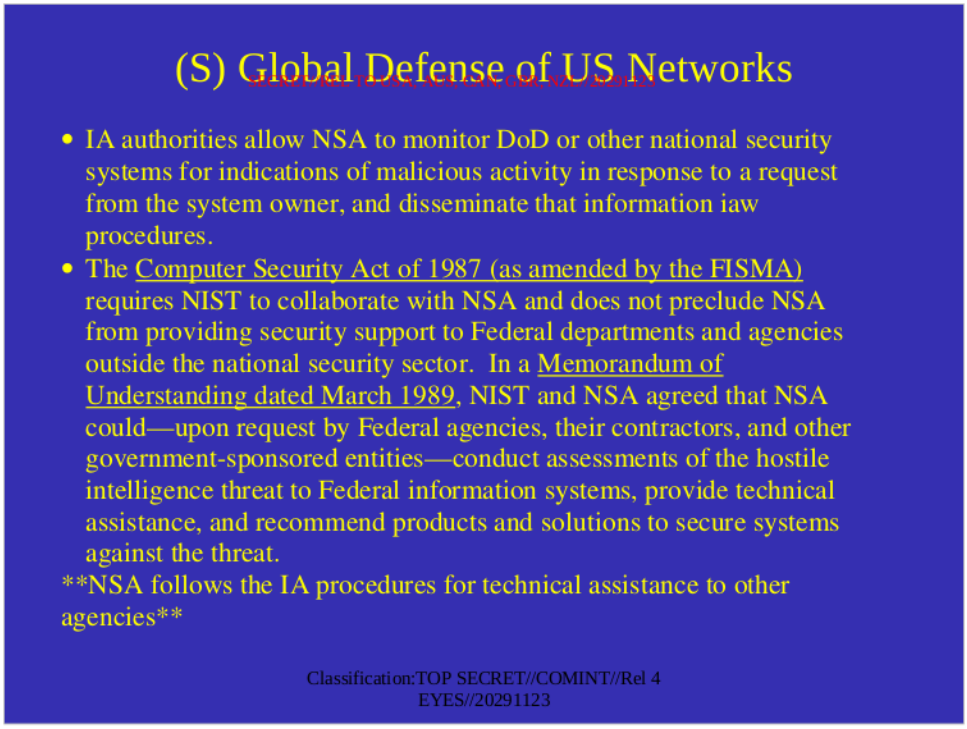
-Disclosure of foreign intrusions to SID is fine under the service provider rules. All foreign comms intrusions into DoD are suspect and can be disseminated for SID to help find out attribution, how intrusion works etc.

-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.

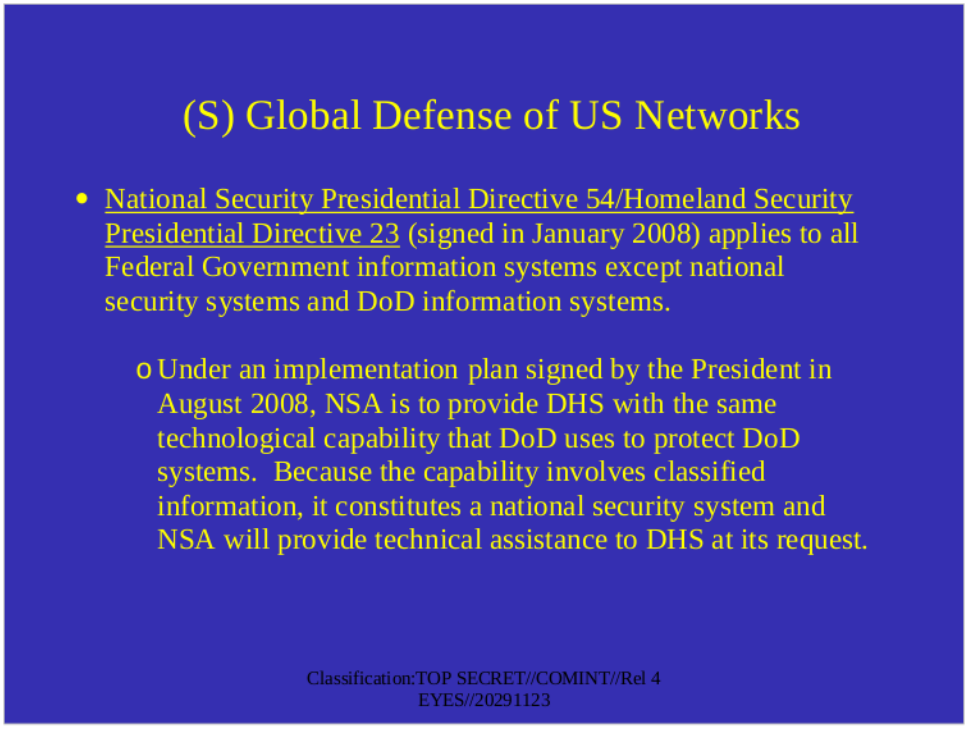
-**The Ground Rules may have different retention periods.

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



-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.



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

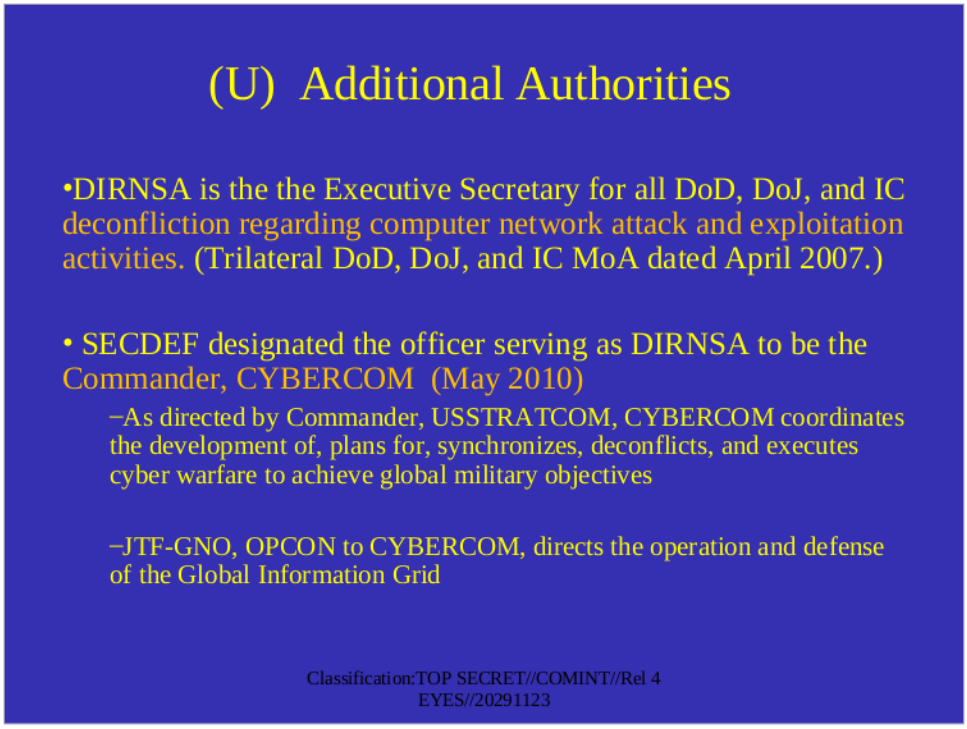
- DHS or other federal agencies can use standard service provider authorities to monitor .gov networks for indications of malicious activity.

- 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.

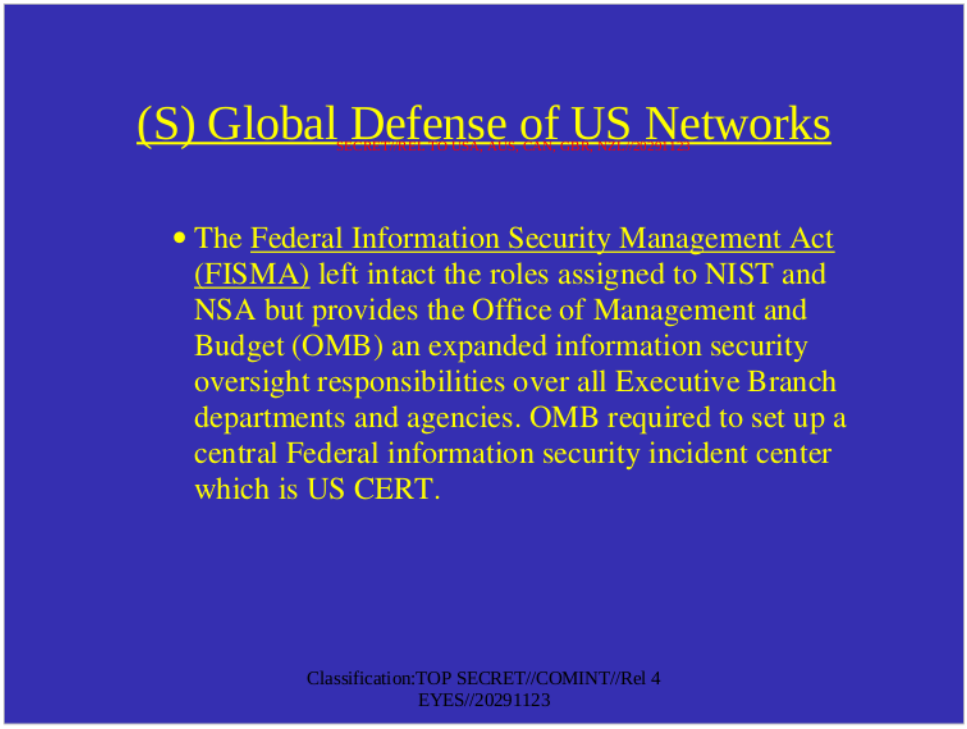
Classification:TOP SECRET//COMINT//Rel 4 EYES//20291123



- 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.



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.



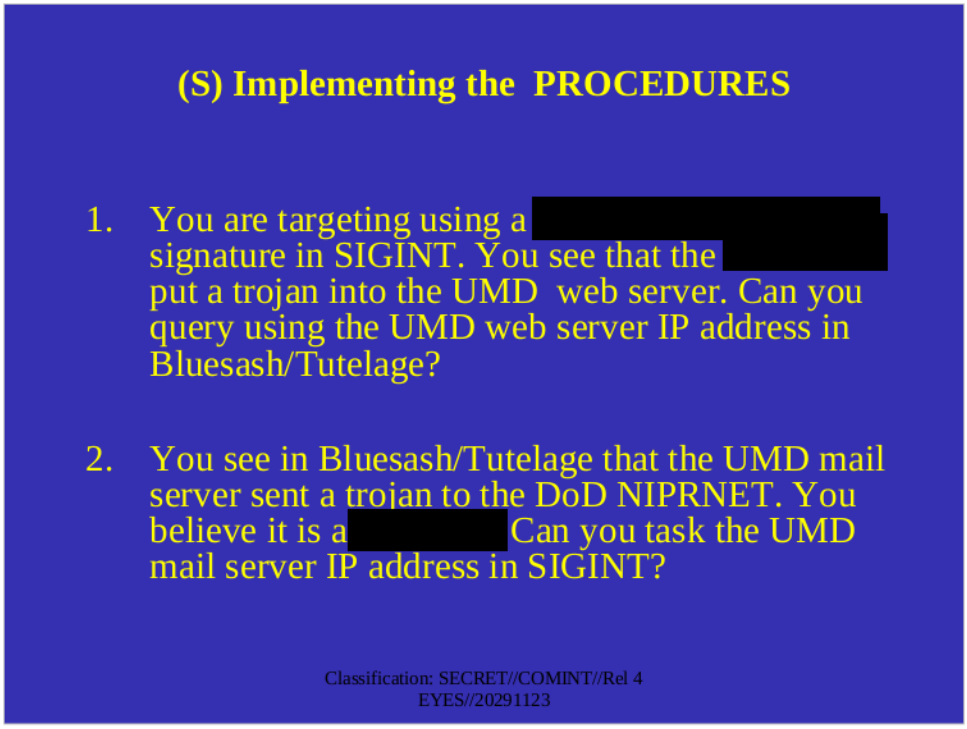
FISMA: 44 U.S.C. 3541 et seq., P.L. 107-347, 116 Stat 2899, 25 November 2002.

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.

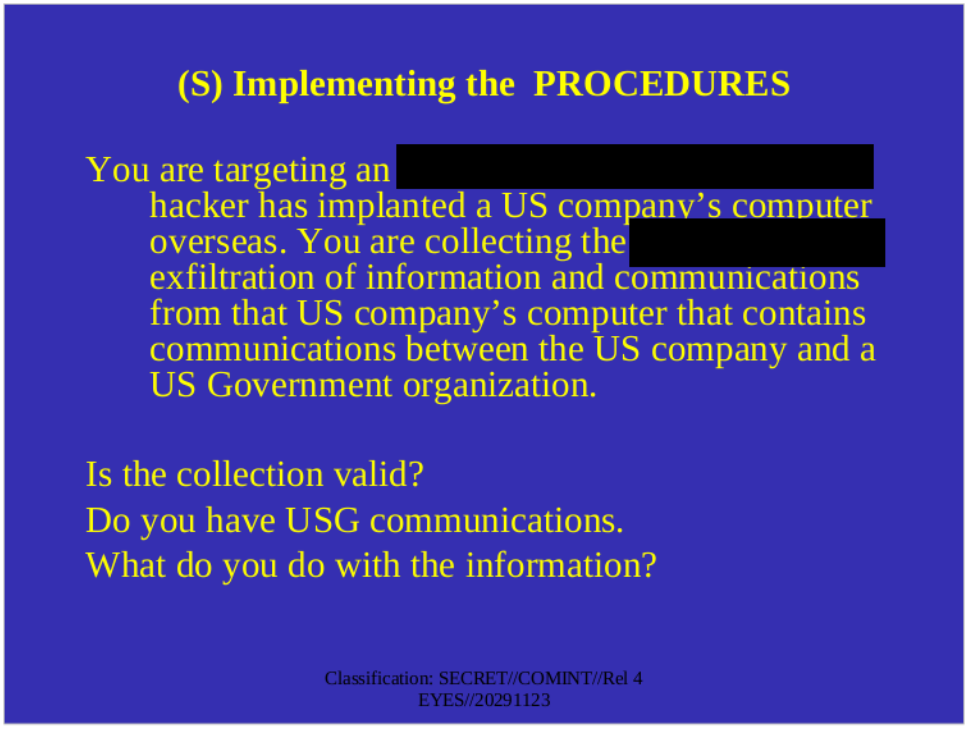
(S) Global Defense of US Networks

- 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.

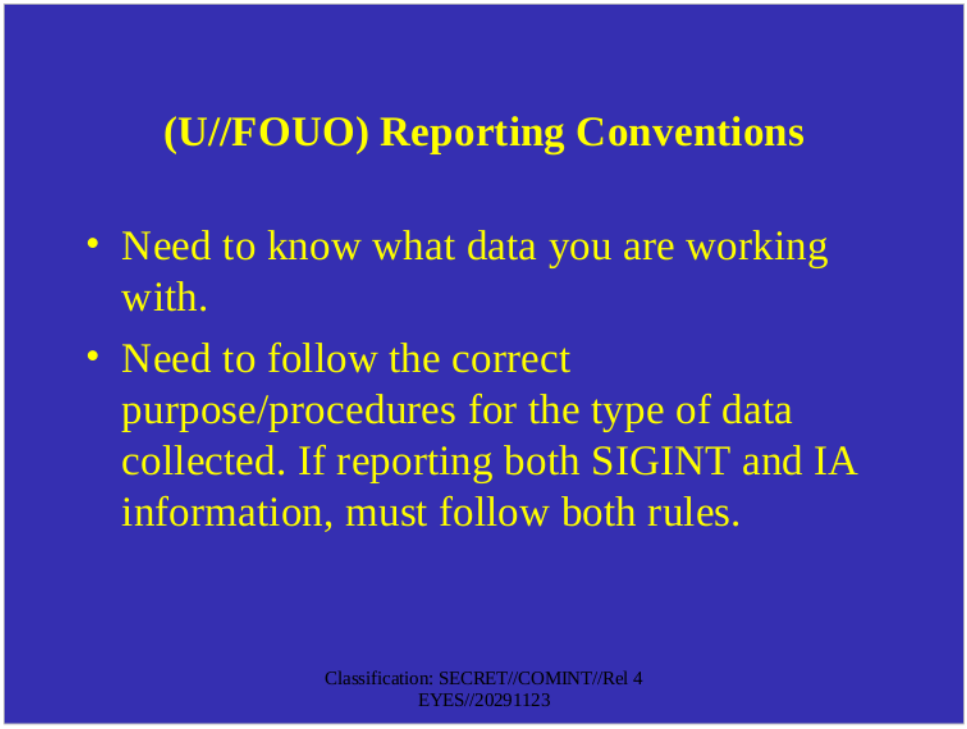
Classification: SECRET//COMINT//Rel 4
EYES//20291123



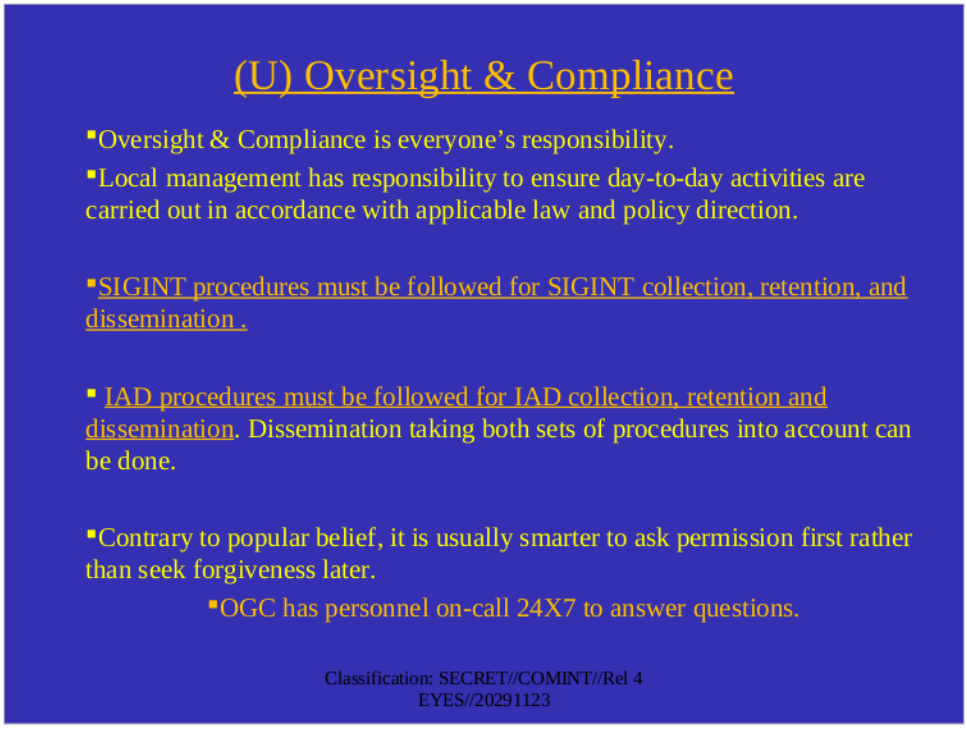
1. Yes, can look for anything suspicious in the IA data to protect the system. The initial SIGINT can be disseminated in a report if it satisfies a FI/CI/SMO requirement. If task the Bluesash/Tutelage deny list, must obtain dissemination approval.
2. No, not as a direct hit but may use a signature in 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 availabe 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.



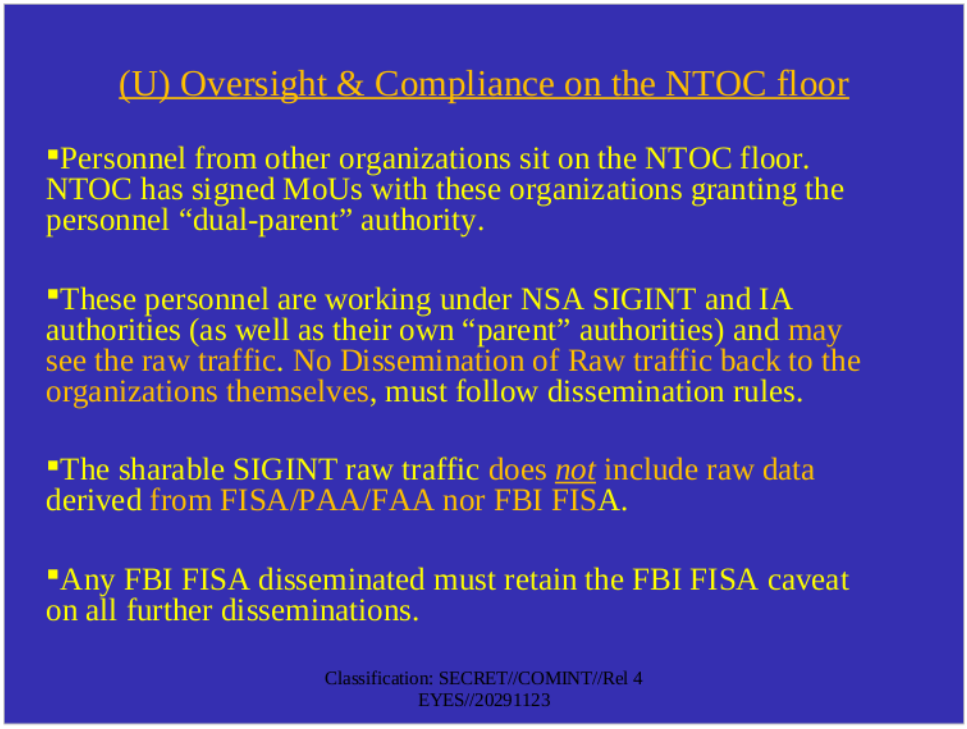
1. Yes, can look for anything suspicious in the IA data to protect the system. The initial SIGINT can be disseminated in a report if it satisfies a FI/CI/SMO requirement. If task the Bluesash/Tutelage deny list, must obtain dissemination approval.
2. No, not as a direct hit but may use a [redacted] signature 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 availabe 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.



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



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



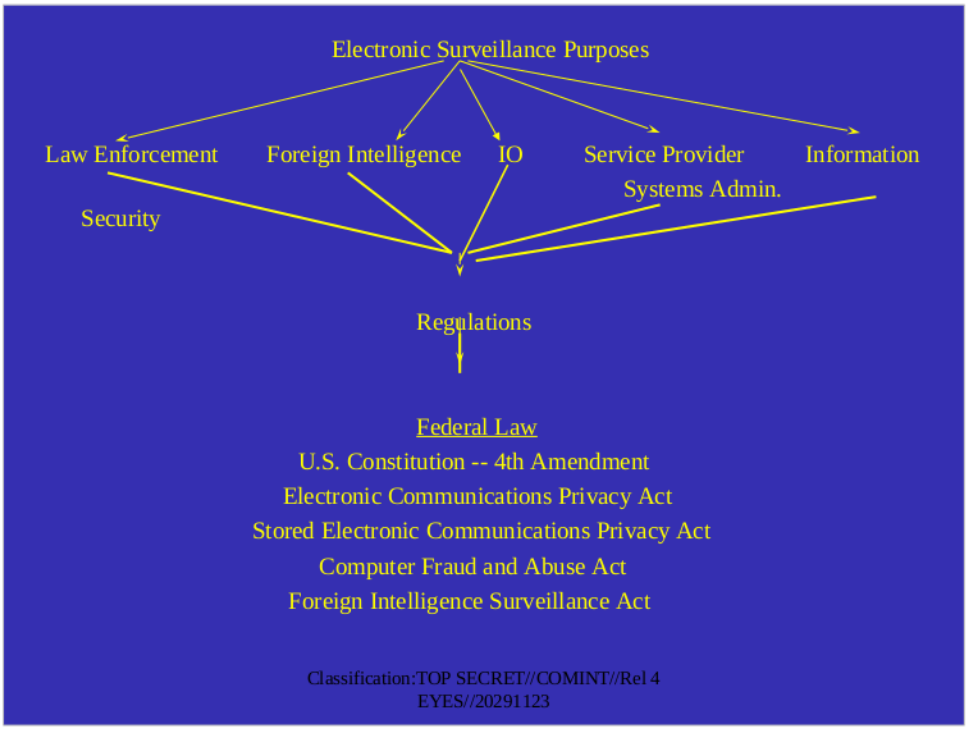
The idea of the NTOC floor is to allow all the personnel on the floor to be able to collaborate, indicate what information is relevant to their organizations mission and facilitate dissemination. However, dissemination back to the organizations themselves is a dissemination and must follow the dissemination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

?????? 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 supoena.]

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
NTISSD 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.

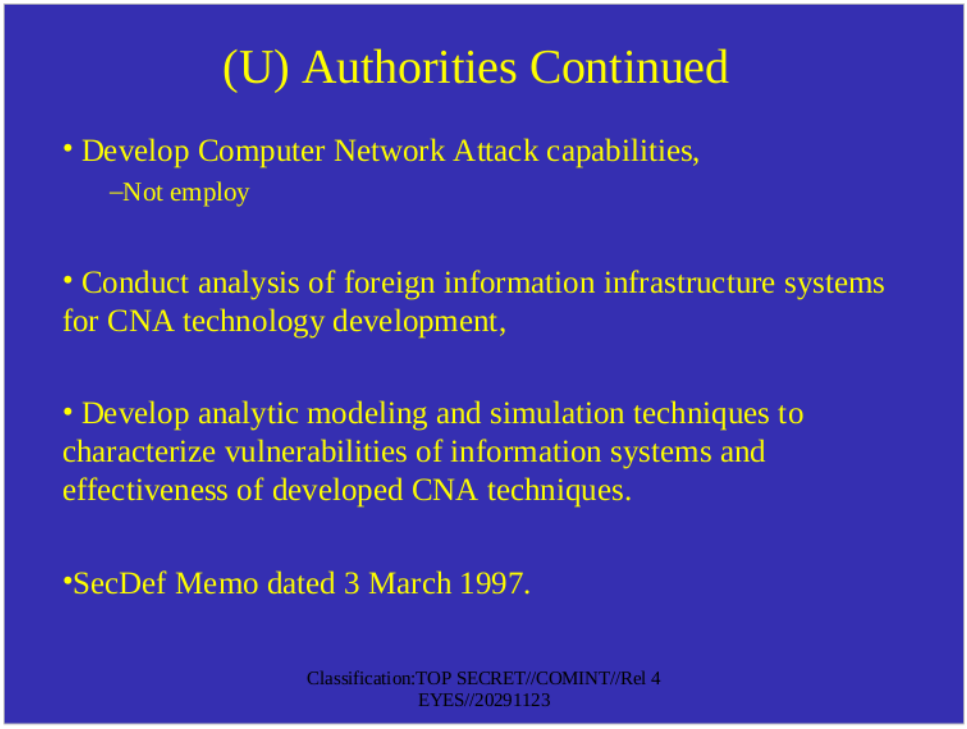
Classification:TOP SECRET//COMINT//Rel 4 EYES//20291123

Used really only by JCMA

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



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



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



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