

TOP SECRET//COMINT//NOFORN



# SSO Corporate Portfolio Overview

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20361201

TOP SECRET//COMINT//NOFORN

TOP SECRET//COMINT//NOFORN



**What is SSO's Corporate  
Portfolio?**

**What data can we collect?**

**Where do I go for more help?**

TOP SECRET//COMINT//NOFORN

Agenda

TOP SECRET//COMINT//NOFORN

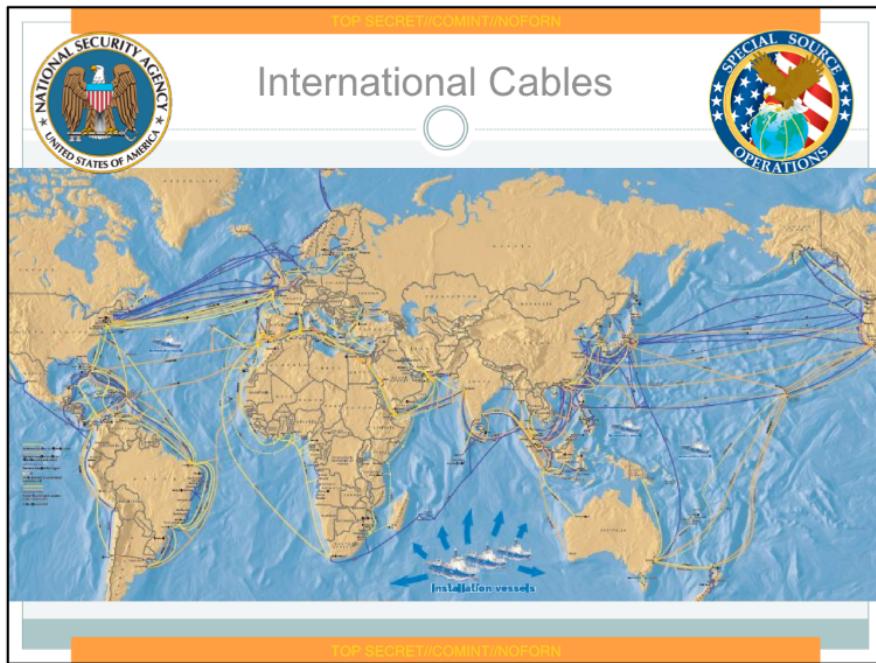


## What is SSO's Corporate Portfolio?

TOP SECRET//COMINT//NOFORN

### **What is SSO Corporate access collection?**

(TS//SI//NF) Access and collection of telecommunications on cable, switch network, and/or routers made possible by the partnerships involving NSA and commercial telecommunications companies.



Brief discussion of global telecommunications infrastructure.

How access points in the US can collect on communications from “bad guy” countries  
(least cost routing, etc.)

TOP SECRET//COMINT//NOFORN



## Unique Aspects



Access to massive amounts of data

Controlled by variety of legal authorities

Most accesses are controlled by partner

Tasking delays

TOP SECRET//COMINT//NOFORN

(TS//SI//NF) Key Points:

- 1) SSO provides more than 80% of collection for NSA. SSO's Corporate Portfolio represents a large portion of this collection.
- 2) Because of the partners and access points, the Corporate Portfolio is governed by several different legal authorities (Transit, FAA, FISA, EO12333), some of which are extremely time-intensive.
- 3) Because of partner relations and legal authorities, SSO Corporate sites are often controlled by the partner, who filters the communications before sending to NSA.
- 4) Because we go through partners and do not typically have direct access to the systems, it can take some time for OCTAVE/UTT/Cadence tasking to be updated at site (anywhere from weekly for some BLARNEY accesses to a few hours for STORMBREW).



Explanation of how we can collect on a call between (hypothetically) Iran and Brazil using Transit Authority.

Discuss how foreign-to-foreignness must be proved (particularly difficult for DNI).

TOP SECRET//COMINT//NOFORN



## Transit Authority



TOP SECRET//COMINT//NOFORN

- (S//SI) Communications must be confirmed foreign-to-foreign.
- (S//SI) Filters at front-ends to ensure only authorized traffic is forwarded to the DNR and DNI selection engines.
- (S//SI) Occasionally the TOPI discovers that one end of the intercept is actually in the US. We refer to this as a "domestic incident".
- (C) TOPI's must inform SSO Corp Team when this occurs via email alias [REDACTED] SSO files a formal report to NSA/SV for each occurrence of a domestic incident.

- (S//SI) Transit Authority – Only allows those SSO programs operating under this authority to collect communications which are confirmed to be foreign-to-foreign.
- (S//SI) SSO programs operating under this authority have filters at their collection front-ends to ensure only authorized traffic (i.e. foreign-to-foreign) is forwarded to the DNR and DNI selection engines (driven by UTT/CADENCE/OCTAVCE tasking).
- (S//SI) Despite best efforts, occasionally there may be an "authorized" DNR or DNI hit forwarded to the TOPI, which based on TOPI analysis eventually determines that one-end of the intercept is actually in the US. We refer to this as a "domestic incident". This usually occurs in the DNR world, where one-end of the intercept will make a reference to being in the US.
- (C) TOPI's must inform SSO Corp Team when this occurs via email alias [REDACTED] SSO files a formal report to NSA/SV for each occurrence of a domestic incident.

Corporate Portfolio			
	FAIRVIEW	OAKSTAR	
(C) US-990	FAIRVIEW	(C) US-3206	MONKEYROCKET*
<u>BLARNEY</u>		(C) US-3217	SHIFTINGSHADOW
(C) US-984	FISA collection	(C) US-3230	ORANGECRUSH
(C) US-984X*	FAA collection	(C) US-3247	YACHTSHOP
<u>STORMBREW</u>		(C) US-3251	ORANGEBLOSSOM
(C) US-983	STORMBREW	(C) US-3273	SILVERZEPHYR
(C) US-3140	MADCAPOCELOT	(C) US-3277	BLUEZEPHYR
<u>SSO Corporate/TAO Shaping</u>		(C) US-3354	COBALTFALCON
(C) US-3105S1	DARKTHUNDER		
(C) US-3105S1	STEELFLAUTA		

Systems under a corporate program can be completely unrelated to one another (e.g., everything in OAKSTAR is different).

\*MONKEYROCKET is expected to become operational in spring 2012.

Blue-colored systems operate under Transit Authority.

US-3150 is an umbrella SSO SIGAD for the Extended Enterprise.

TOP SECRET//COMINT//NOFORN



## US-990 FAIRVIEW



TOP SECRET//COMINT//NOFORN

(TS//SI) US-990 (PDDG-UY) – key corporate partner with access to international cables, routers, and switches.

(TS//SI) Key Targets: Global

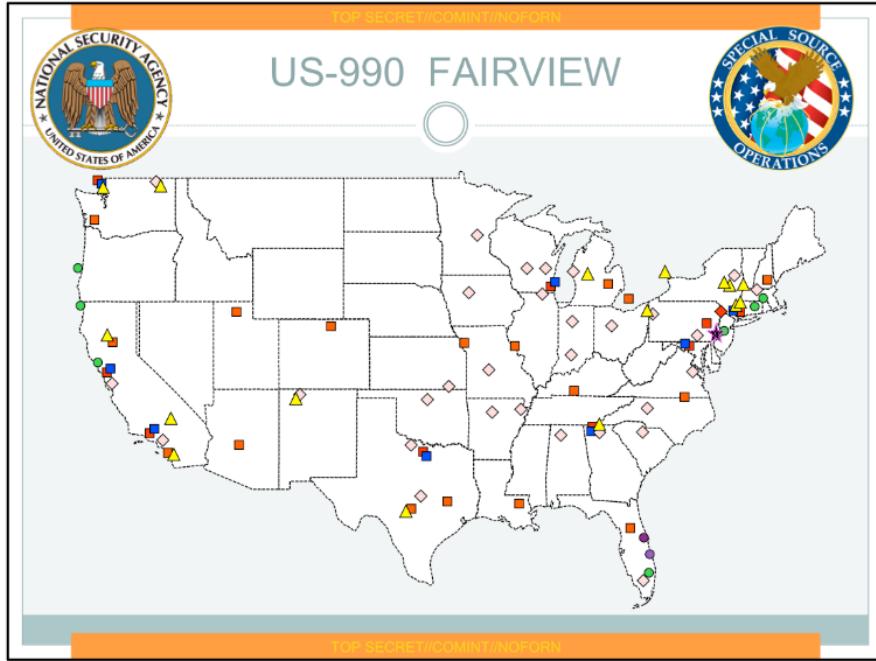
(C) DNR: Directory ONMR

(C) DNI: Port 25 only under Transit Authority  
All port traffic under FAA Authority  
Cyber access

TOP SECRET//COMINT//NOFORN

Key points:

- 1) Explanation of Port 25 and 3-Swing Algorithm.
- 2) 60 million foreign-to-foreign emails in the FAIRVIEW environment ever day; 5 million after 3-Swing Algorithm.
- 3) FAA collection under SIGADs US-984XR and US-984X2. FISA collection under SIGAD US-984T (COWBOY).
- 4) Tasking through UTT, Cadence, and OCTAVE.
- 5) Data in PINWALE (YANKEE), XKEYSCORE, MAINWAY, TOYGRIPPE, BLACKPEARL, TWISTEDPATH, NUCLEON, and DISHFIRE.



Discussion of the breadth of the FAIRVIEW program.

TOP SECRET//COMINT//NOFORN



## US-983 STORMBREW



(TS//SI) US-983 (PDDG-FL) – key corporate partner with access to international cables, routers, and switches

(TS//SI) Key Targets: Global

(C) DNR Collection: (Directory ONMR)

(C) DNI Collection: Limited to FAA and FISA  
Cyber hit counts on FAA DNI Access

TOP SECRET//COMINT//NOFORN

**Key Points:**

- 1) Access to mid-point collection (cable, switch, and router) at seven sites and approximately 130 circuits.
- 2) DNR collection falls under Transit and FAA Authorities. DNI is limited to FAA and FISA – cannot collect DNI under Transit Authority like FAIRVIEW.
- 3) Difference between WHITESQUALL (international gateway switch access; thousands of trunk groups connected worldwide), MISTRALWIND (calling card/ private network access), SERRATEDEDGE (conflict number access)
- 4) STORMBREW collects under the FAA Authority using the SIGADs US-984X(A-H) for DNI and US-984X1.
- 5) STORMBREW handles limited FISA-related tasking using the SIGAD US-984P (PERFECTSTORM) and PDDG AX.
- 6) STORMBREW is tasked in UTT and OCTAVE.
- 7) Data is retrieved in PINWALE, NUCLEON, and DISHFIRE.



(TS//SI//NF) STORMBREW collection comes from eight sites connected by a DS3 ring.

TOP SECRET//COMINT//NOFORN



**US-3140 MADCAPOCELOT**

(TS//SI) US-3140 (PDDG: TM) – Target DNI operating under E.O. 12333 Authority.

(TS//SI) Key Targets: [REDACTED]  
[REDACTED]

(S) DNI and metadata through XKEYSCORE, PINWALE, and MARINA.

TOP SECRET//COMINT//NOFORN

- 1) New access under the STORMBREW umbrella.
- 2) MADCAPOCELOT has access to multiple 10G internet backbone circuits, including several that service the [REDACTED]
- 3) Three-step tasking process: 1) an unclassified IP address and signature promotion list will be reviewed and approved by S2/S3 GCM equity process, 2) strong selection will be accomplished by UTT site group (SSO\_WO), 3) filtering and targeting logic managed by TMM will be levied via a new CADENCE dictionary MADCAPOCELOT and CADENCE FIST MDCP.
- 4) Collection can be accessed in PINWALE (TEXT partition) and metadata is accessed in MARINA.

TOP SECRET//COMINT//NOFORN



**US-984 BLARNEY**



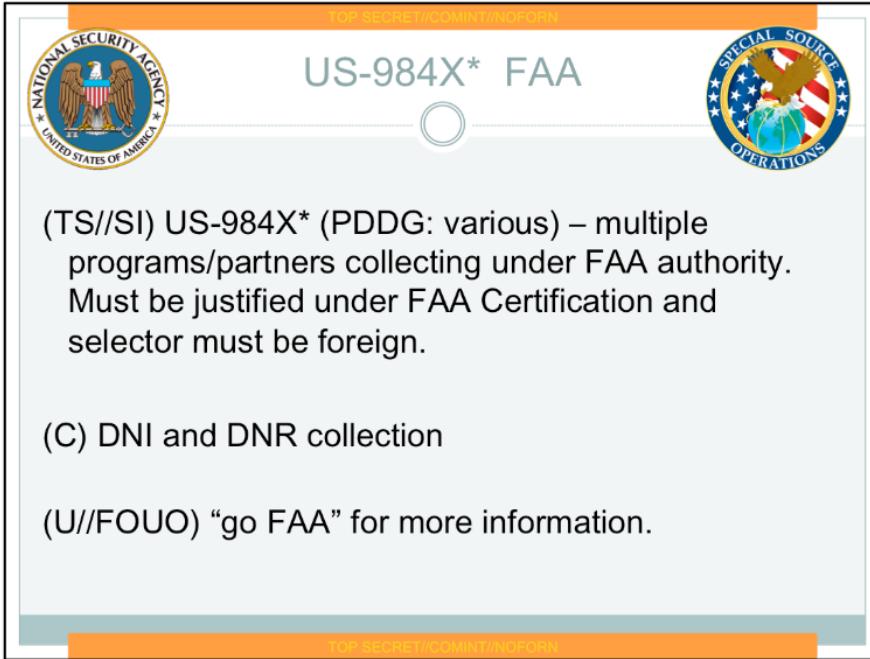
(TS//SI) US-984 (PDDG: AX) – provides collection against DNR and DNI FISA Court Order authorized communications.

(TS//SI) Key Targets: Diplomatic establishment, counterterrorism, Foreign Government, Economic

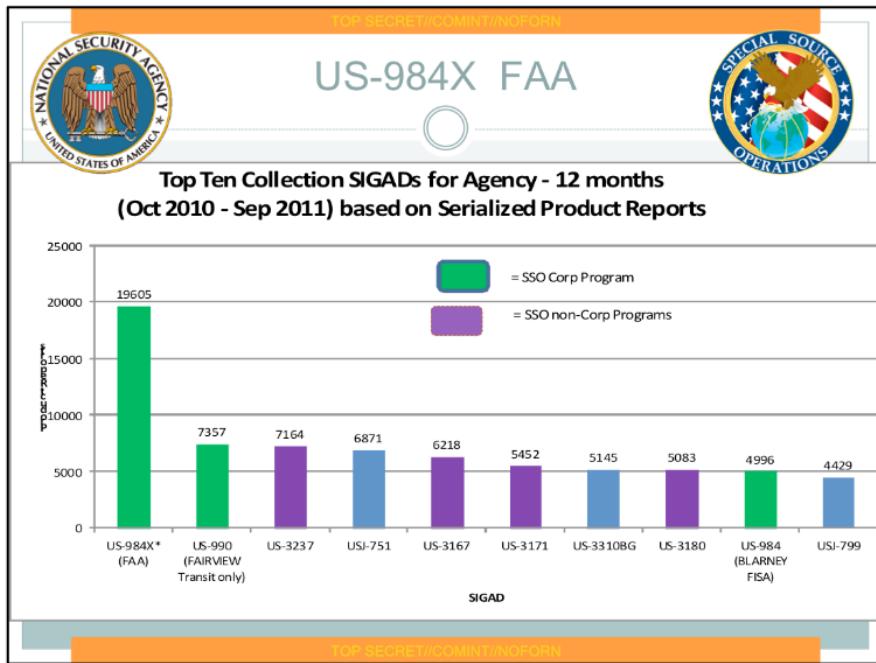
(U//FOUO) “go BLARNEY” for more information.

TOP SECRET//COMINT//NOFORN

- 1) Operates under the authorities of NSA FISA, FBI FISA, and FAA.
- 2) BLARNEY is the leading source of FISA collection, producing over 11,000 reports and is consistently a top contributor to the President's Daily Brief. The program contributes to over 60% of product reporting to the Counterterrorism product line and over 80% of the overall FAA reporting.
- 3) In order to task BLARNEY, there must be a valid Court Order for the target. Court order process:
  - 1) Court Order is signed or renewed.
  - 2) Selectors appear in the Court Order.
  - 3) Target Office decides what numbers to task. The Target Office submits a task request (via email to [REDACTED]) to the BLARNEY Collection Managers with the selectors that should be tasked.
  - 4) When a Court Order is up for renewal and a currently tasked number is not going to be in the renewal, the TOPI is required to send a detask request for that selector.
- 4) 11 different SIGADs, falling under BLARNEY, FAIRVIEW, and STORMBREW partners.
- 5) PRISM falls under BLARNEY, but is just one access of many.
- 6) The Court Order process is extremely long and time-intensive for everyone involved, but the collection payout is fantastic.



- 1) FAA Collection falls under BLARNEY, FAIRVIEW, STORMBREW, or SILVERZEPHYR (OAKSTAR), but due to the stringent legal requirements of FAA, the programs use different SIGADs (under the format US-984X\*).



Look at FAA. Just look at it.



# US-3206 MONKEYROCKET



(TS//SI) US-3206 (PDDG: 6T) – Operates from a foreign access point under E.O. 12333.

(C) Expected IOC: Spring 2012

(TS//SI) Key Targets: CT-focused – Middle East, Europe, and Asia

(S//SI) DNI Metadata & Content