



FAIRVIEW

SSO FAIRVIEW Overview

FAIRVIEW

AGENDA

- (U) FAIRVIEW DEFINED
- (U) OPERATIONAL AUTHORITIES/CAPABILITIES
- (U) STATS: WHO IS USING DATA WE COLLECTED
- (U) FAIRVIEW WAY AHEAD AND WHAT IT MEANS FOR YOU
- (U) QUESTIONS

FAIRVIEW

International Cables

(TS//SI//NF)



(TS//SI//NF)



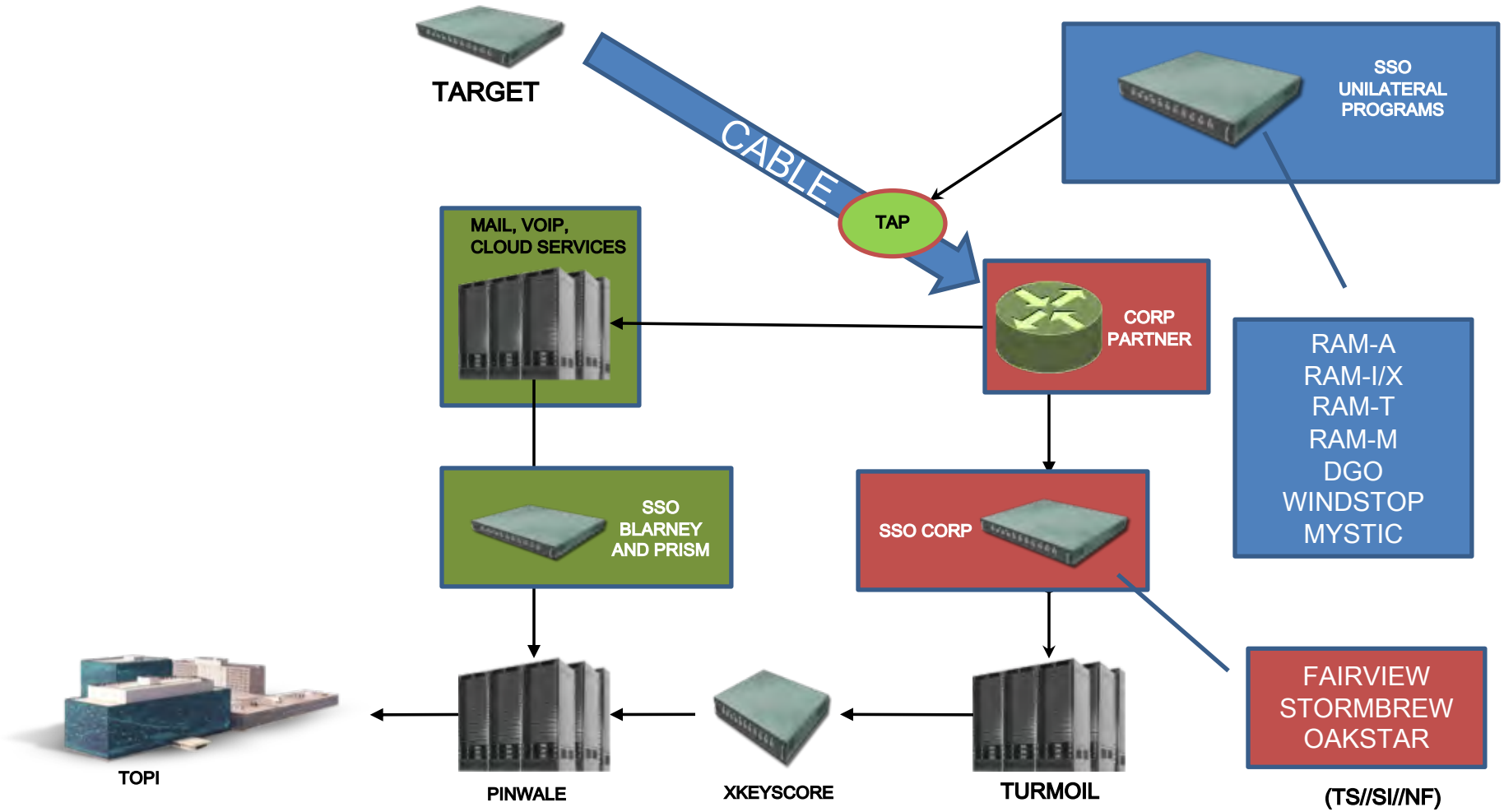
Brief discussion of global telecommunications infrastructure.

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

FAIRVIEW

WHERE SSO IS ACCESSING YOUR TARGET

(TS//SI//NF)



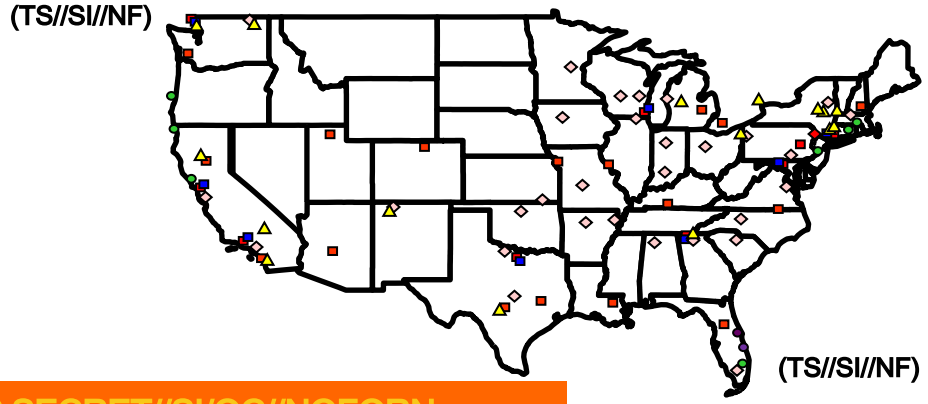
FAIRVIEW

FAIRVIEW DEFINED

- (TS//SI//NF) Large SSO Program involves NSA and Corporate Partner (Transit, FAA and FISA)

- (TS//SI//REL FVEY) Cooperative effort associated with mid-point collection (cable, switch, router)

- (TS//SI//NF) The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs



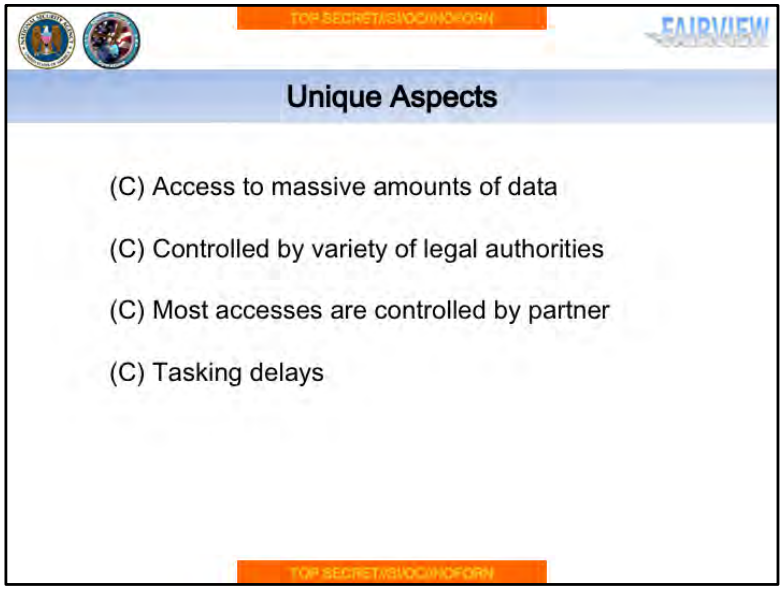
Unique Aspects

(C) Access to massive amounts of data

(C) Controlled by variety of legal authorities

(C) Most accesses are controlled by partner

(C) Tasking delays



(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).

FAIRVIEW

Transit Authority

(TS//SI//NF)



(TS//SI//NF)

FAIRVIEW

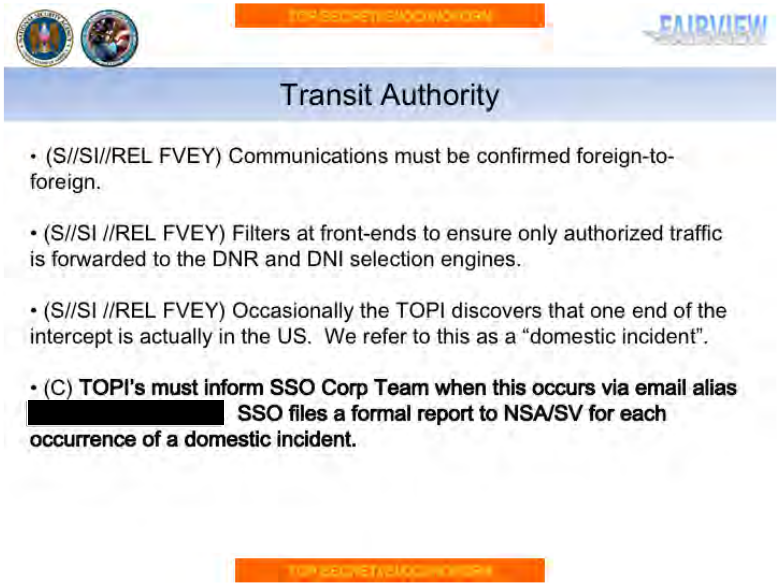
Transit Authority

• (S//SI//REL FVEY) Communications must be confirmed foreign-to-foreign.

• (S//SI //REL FVEY) Filters at front-ends to ensure only authorized traffic is forwarded to the DNR and DNI selection engines.

• (S//SI //REL FVEY) 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 [redacted]. SSO files a formal report to NSA/SV for each occurrence of a domestic incident.**

FAIRVIEW

US-990 FAIRVIEW-TRANSIT

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

(TS//SI//NF) Key Targets: Global

(C) DNR: Directory ONMR

(C) DNI: Port 25 only under Transit Authority

All port traffic under FAA Authority

Cyber access



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.

FAIRVIEW

US-984X* - FAA

(TS//SI//NF) US-984XR (PDDG: YC-DNI) and US-984X2 (PDDG: 29-DNR) –collecting under FAA authority. Must be justified under FAA Certification and selector must be foreign.

(C) DNI and DNR collection

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

FAIRVIEW

US-984T - FISA

(TS//SI//NF) US-984T– Must be justified under FISA warrant.

(C) DNI collection

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

FAIRVIEW

FAIRVIEW Targeting Capabilities

FAA SMS Targeting

- (TS//SI// REL FVEY) DISHFIRE/SPYDER are not partitioned to support FAA SMS targeting
- (TS//SI//NF) Category: 4208 SIGAD: US-984X2
- (TS//SI// REL FVEY) Data can be found in PINWALE
- (TS//SI// REL FVEY) Began APR/MAY 2011

FAA IP Targeting

- (TS//SI//NF) If you know an IP is foreign and all actors using that IP is a valid target, then it can be tasked via UTT
- (TS//SI//REL FVEY) 25 IPs tasked through UTT
- (TS//SI//NF) Collect anything coming from that IP

(TS//SI//NF)

IP addresses approved for 702 tasking	IP Subnet Filter	Target	Date of DOJ/ODNI pre-approval
[redacted]	Yes	[redacted]	30-Jul-12
[redacted]	Yes	Faded Aftermath	24-Jul-12
[redacted]	Yes	CARBONFURY	30-Aug-12
[redacted]	Yes	[redacted]	2-Feb-13

(TS//SI//NF)

FAIRVIEW

US-3105S1 FAIRVIEW/TAO Shaping

(TS//SI//REL FVEY) US-3105S1 (PDDG: DU) - FAIRVIEW support to Tailored Access Office (TAO) shaping operations collecting under E.O. 12333 authority

* NATIVEFLORA –
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) (DNI collection)

* UNICORNSANDWICH –
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) (DNI collection)

* CROSSEYEDBEAR –
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) (DNI collection)

* SCORCHERSIX –
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) (DNI collection)

* TROPICTHUNDER –
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) (DNI collection)

* DARKTHUNDER – **SUSPENDED**
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) DNI collection

* STEELFLAUTA – **SUSPENDED**
Case Notation: [redacted]
(TS//SI) Key Targets: [redacted]
(S//SI) DNI collection

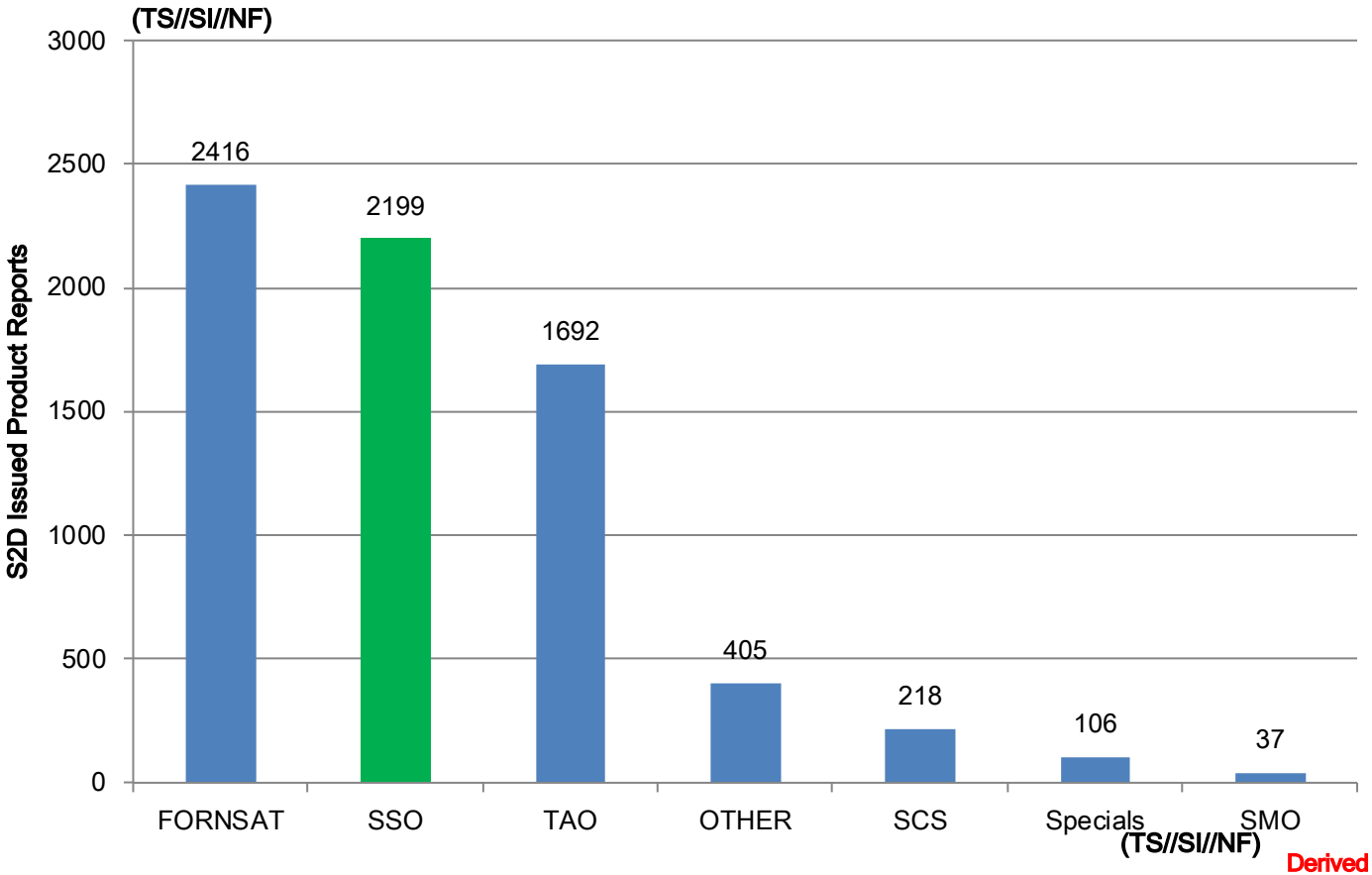
Note: Expect more TAO/SSO shaping efforts in near future.

FAIRVIEW

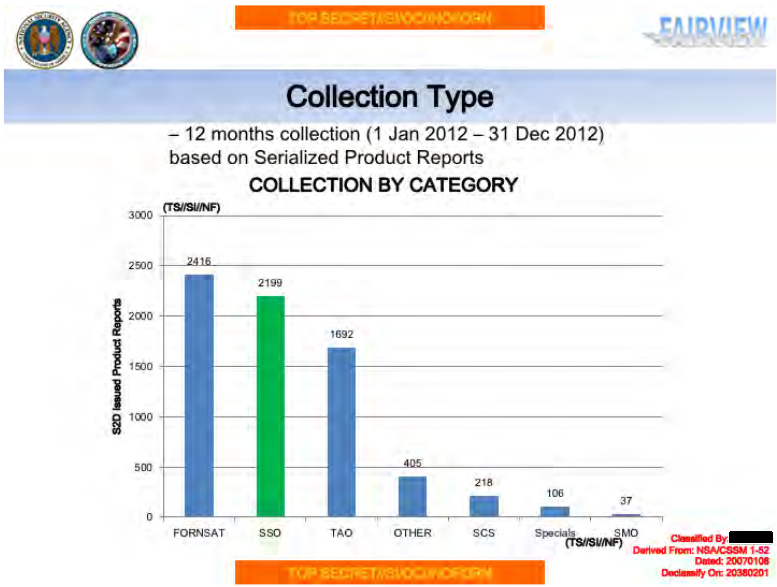
Collection Type

– 12 months collection (1 Jan 2012 – 31 Dec 2012) based on Serialized Product Reports

COLLECTION BY CATEGORY



Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380201



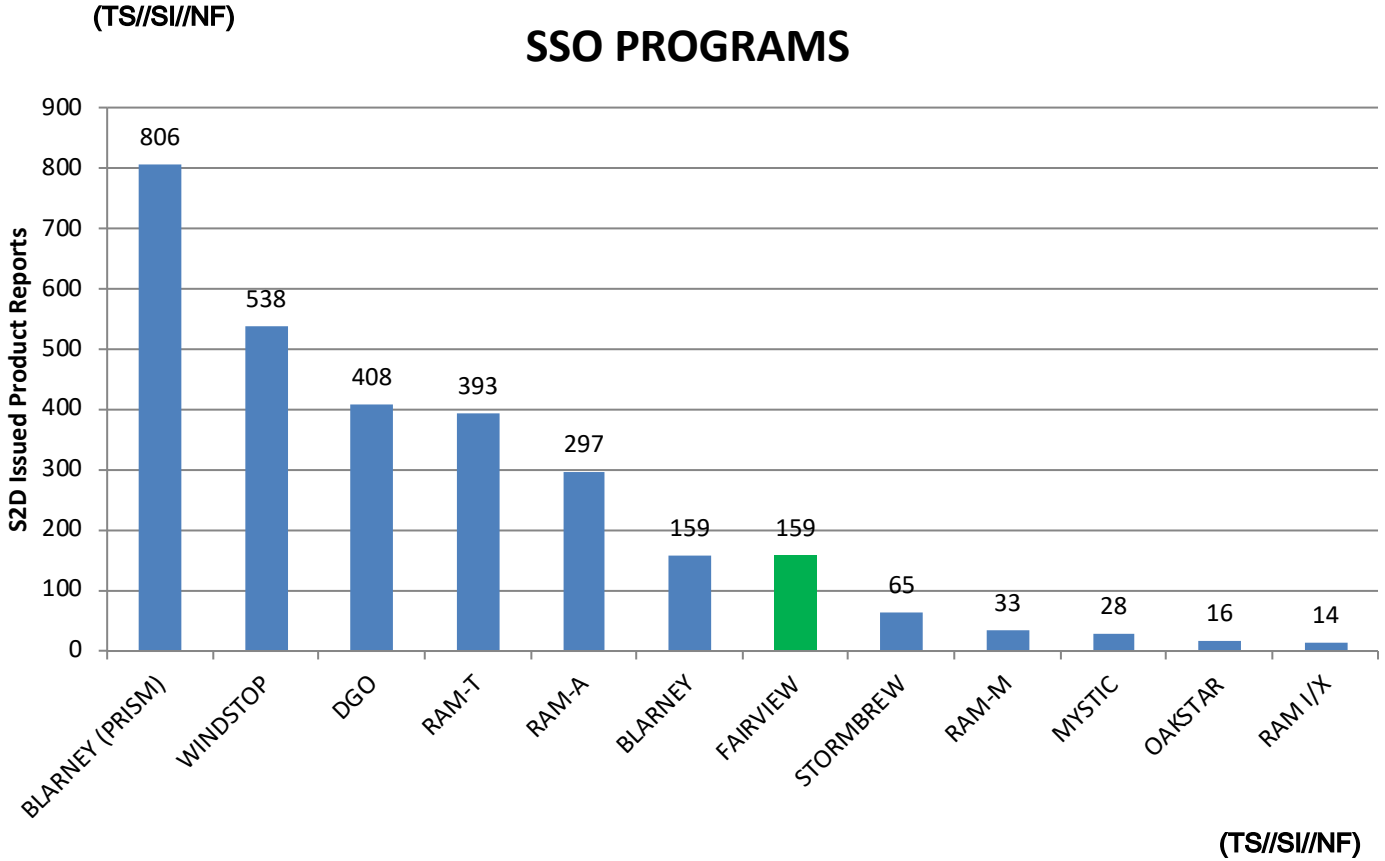
Look at FAA. Just look at it.

FAIRVIEW

SSO Programs

– 12 months of collection (1 Jan 2012 – 31 Dec 2012)
based on Serialized Product Reports

(TS//SI//NF)



(TS//SI//NF)

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380201



Look at FAA. Just look at it.

SSO Corp Programs Support to S2D

(TS//SI//NF) SSO-FAIRVIEW Programs contributed to 159 S2D Product Reports in 2012. This represented ~1.4% of total S2D Product Reports for 2012.



(TS//SI//NF) 159 PRODUCT REPORTS ATTRIBUTED TO FAIRVIEW. 11’591 PRODUCTS PRODUCED BY S2D IN 2012.

FAIRVIEW

SSO Corp Support to S2D

(TS//SI//NF)

SSO Corp Program	S2D1 Product Reports	S2D2 Product Reports	S2D3 Product Reports	S2D4 Product Reports
BLARNEY US-984* (less US-984X*)	12	2	151	-
PRISM (US-984XN)	273	291	150	35
US-984X* FAA (not US-984XN)	286	340	164	35
STORMBREW (US-983)	27	4	7	3
FAIRVIEW (US-990)	**46**	**13**	**21**	**9**
OAKSTAR (US-3277, US-3354, US-3206, US- 3251, US-3230, US-3217, US-3273, US-3333, US-3247)	9	-	7	2
STORMBREW (US-984XA-XH)	18	22	2	-
FAIRVIEW (US-984XR, US-984X2)	**17**	**43**	**18**	**-**
STORMBREW (US-984P)	-	-	-	-
FAIRVIEW (US-984T)	**-**	**-**	**-**	**-**
Total Serialized Product Reports	411	401	329	48

(TS//SI//NF)

FAIRVIEW

FAA DNI Tasking (30 Jan)

(TS//SI//NF)

Product Line	All DNI Selectors Tasked	DNI Selectors Tasked to SSO_CT_N (FAA/PRISM)	% of DNI Selectors Tasked to FAA/PRISM	% Points Change From Dec 2011	Increase in number of selectors tasked to FAA/PRISM Compared to Dec2011
S2A	9650	987	10%	**-5**	**+232**
S2B	12872	2263	18%	**+6**	**+842**
S2C	8763	1059	12%	**+3**	**+468**
S2D	**10846**	**3796**	**35%**	**+11**	**+1872**
S2E	18061	6935	38%	**-4**	**+938**
S2F	3577	1011	28%	**+2**	**+423**
S2G	12788	4172	33%	**+2**	**+1019**
S2H	10497	828	8%	**+6**	**+660**
S2I	14945	11461	77%	**-1**	**+818**
S2J	1077	242	22%	**-2**	**-55**

(TS//SI//NF)

FAIRVIEW

TOPI Access To FAA Data

- (TS//SI//NF) Analysts must have FAA training and RAGTIME – A & C access to view all the data
- (TS//SI//NF) SSO Corporate FAA DNI traffic is available in PINWALE under the SWEETSMACK2 (CT) SOURSMACK2 (FG, CP) partitions/visibility groups
- (TS//SI//NF) FAIRVIEW FAA DNR data is accessible to all in NUCLEON, SIGAD = US-984X2

FAIRVIEW CAPABILITIES AND WAY AHEAD

- (TS//SI//NF) FAIRVIEW is using the EVILOLIVE list as front-end filter, which gives the widest aperture to pull traffic into TURMOIL
  - SCALEABLE – expanding with addition of IPv6
  - FLEXIBLE – SSO updated daily
  - Dynamic – filters updated every 2 weeks but can be updated within 24 hrs if required

- (TS//SI//NF) FAIRVIEW transit DNI is developing capability to expand to POP3

- (TS//SI//NF) FAIRVIEW transit DNR safeguards –
  - number normalization (OPC/DPC) – REGEX rules
  - TOPIs are the last line of defense in reporting one-end domestic incidents to SSO and requesting data purge
  - SSO improving processes for reporting infractions and implementing fixes

FAIRVIEW

Corporate Portfolio

FAIRVIEW

(C) US-990	FAIRVIEW (T)
(C) US-984XR	FAIRVIEW (FAA)
(C) US-984X2	FAIRVIEW (FAA)
(C) US-984T	FAIRVIEW (FISA)

BLARNEY

(C) US-984	FISA collection
(C) US-984X*	FAA collection

STORMBREW

(C) US-983	STORMBREW (T)
(C) US-984XA-H	STORMBREW (FAA)
(C) US-984P	STORMBREW (FISA)

OAKSTAR

(C) US-3206	MONKEYROCKET*
(C) US-3217	SHIFTINGSHADOW
(C) ~~US-3230~~	~~ORANGECRUSH~~
(C) US-3247	YACHTSHOP
(C) US-3251	ORANGEBLOSSOM
(C) ~~US-3273~~	~~SILVERZEPHYR (T/FAA)~~
(C) US-3277	BLUEZEPHYR
(C) US-3354	COBALTFALCON

SSO Corporate/TAO Shaping

(C) US-3105S1

T= Transit



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

*MONKEYROCKET is expected to become non-operational at the end of 2013.

Blue-colored systems operate under Transit Authority.

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

FAIRVIEW

Help Us Help You

• (TS//SI//REL FVEY) Submit Surrey Requirements to Unconventional Collection Discipline, with US-990 as a nominated SIGAD. (Protect your accesses)

• (TS//SI//REL FVEY) Task FAIRVIEW in CADENCE dictionaries and UTT (we have ~5 million emails/day that make it past our authorization process and which then get sent to our dictionaries to see if any are tasked by our customers).

• (TS//SI//REL FVEY) Accurate inclusion of Case Notation in reporting records. Permits us to backtrack and determine productive links and keep them on copy.

• (TS//SI//REL FVEY) General Feedback – things going right (gee-whiz products which FV contributed to), things that can be improved.

• (TS//SI//REL FVEY) Take advantage of FAA tasking. If you can justify it under existing FAA Certifications, you should be tasking your selectors under FAA authority. This opens up the FAIRVIEW program to do more than just port-25 collection (which is what we only do under Transit Authority).

FAIRVIEW

Contact Us

Collection Managers

FAIRVIEW [redacted]

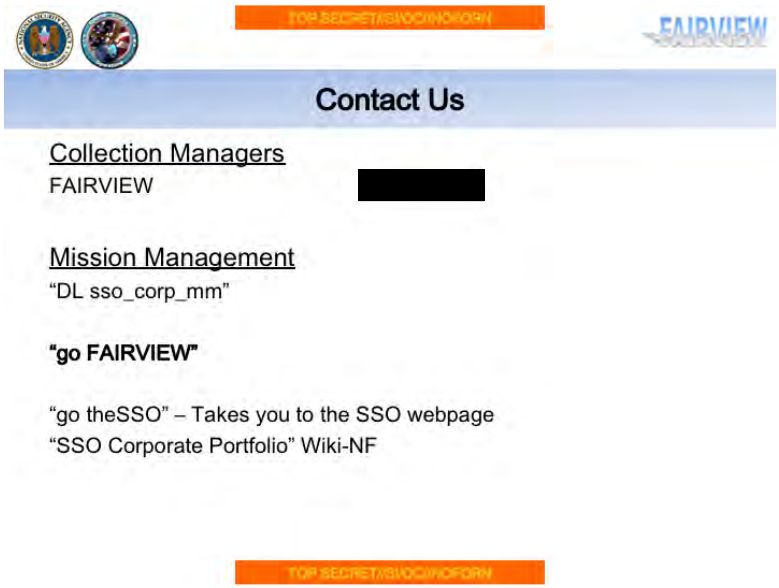
Mission Management

“DL sso_corp_mm”

“go FAIRVIEW”

“go theSSO” – Takes you to the SSO webpage

“SSO Corporate Portfolio” Wiki-NF



1) Questions about individual accesses should be sent to the appropriate collection manager.
2) Questions about tasking should be sent to Mission Management.
3) All the information in this brief (in much more detail) can be found on the SSO Corporate Portfolio pages on WIKI-NOFORN.

Questions?