



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?

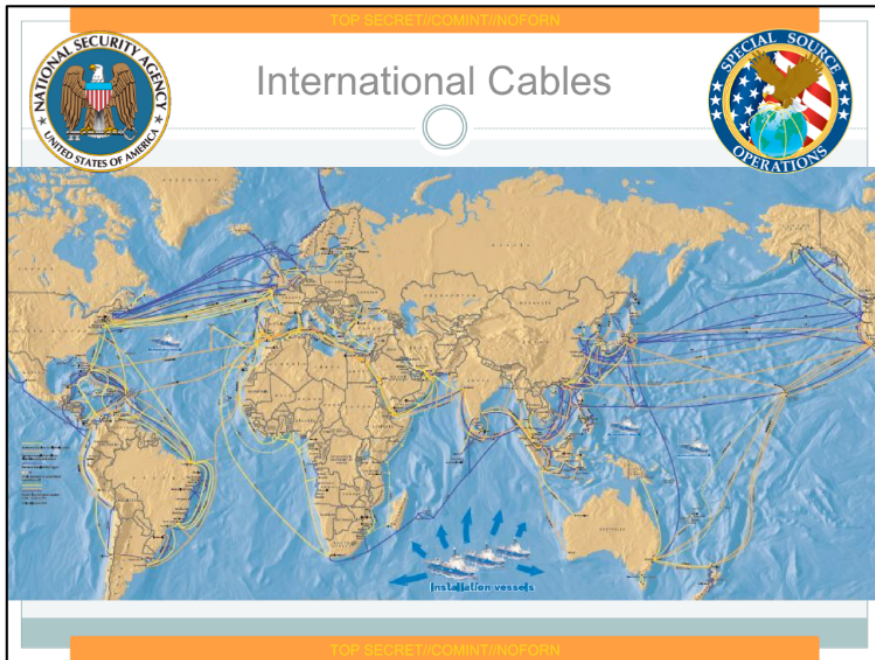
TOP SECRET//COMINT//NOFORN

Agenda



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//SI//NF//NOFORN



Unique Aspects



TOP SECRET//SI//NF//NOFORN

- Access to massive amounts of data
- Controlled by variety of legal authorities
- Most accesses are controlled by partner
- 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).




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//SI//NF//NF//NF



Transit Authority




- (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.**


TOP SECRET//SI//NF//NF//NF

- (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.**

TOP SECRET//SI//NF//NOFORN



Corporate Portfolio



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

TOP SECRET//SI//NF//NOFORN


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//SI//NF//NOFORN



US-990 FAIRVIEW



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

(TS//SI) Key Targets: Global

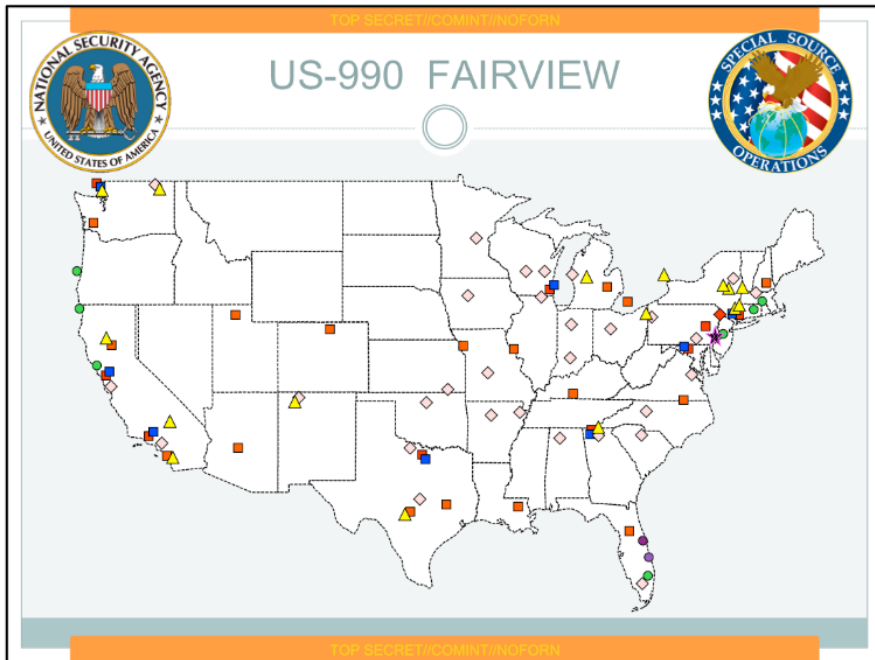
(C) DNR: Directory ONMR

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

TOP SECRET//SI//NF//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//SI//NF//NF//NF



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//SI//NF//NF//NF


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), SERRATEDEGE (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//SI//NF//NOFORN



US-3140 MADCAPOCELOT



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


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

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


TOP SECRET//SI//NF//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//SI//NF//NF



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//SI//NF//NF

- 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 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.

TOP SECRET//SI//NF//NOFORN



US-984X* FAA



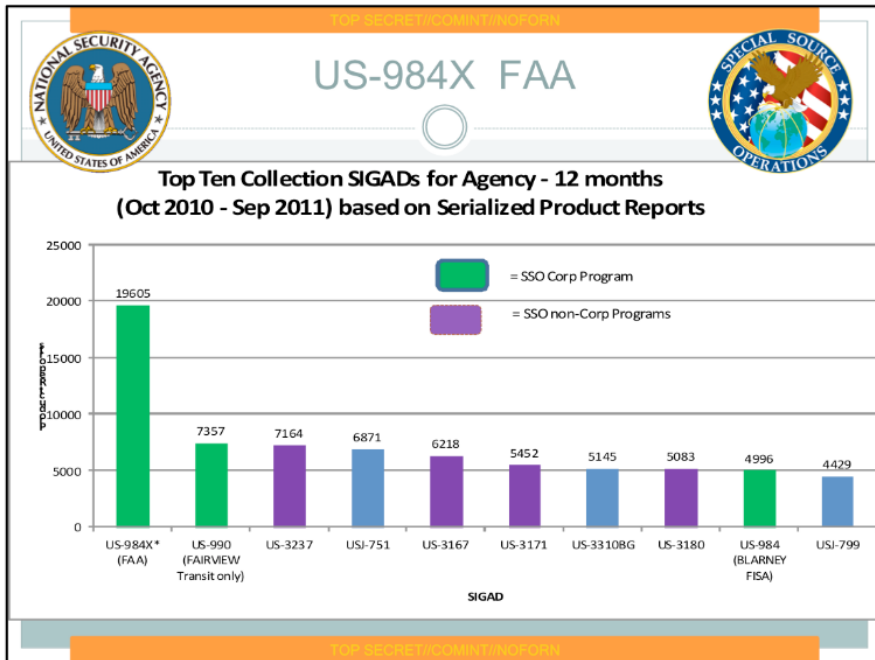
(TS//SI) US-984X* (PDDG: various) – multiple programs/partners collecting under FAA authority. Must be justified under FAA Certification and selector must be foreign.

(C) DNI and DNR collection

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

TOP SECRET//SI//NF//NOFORN

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.



TOP SECRET // COMINT // NOFORN//20291130



Special Source Operations

Corporate Partner Access

Briefed by: [REDACTED]



TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130



**Overall Briefing Classification Is
TOP SECRET//COMINT//NOFORN//X1**

TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130



Relationships & Authorities

- Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routers throughout the world
- Collection on U.S. soil is conducted under three different authorities:
 - Transit Authority: Collection of foreign intelligence communications which originate and terminate in foreign countries, but traverse U.S. territory
 - Foreign Intelligence Surveillance Act (FISA): Court ordered collection (NSA/FBI/FISA Court)
 - FISA Amendment Act of 2008 (FAA): Surveillance in the US when the target is reasonably believed to be foreign

TOP SECRET // COMINT // NOFORN//20291130

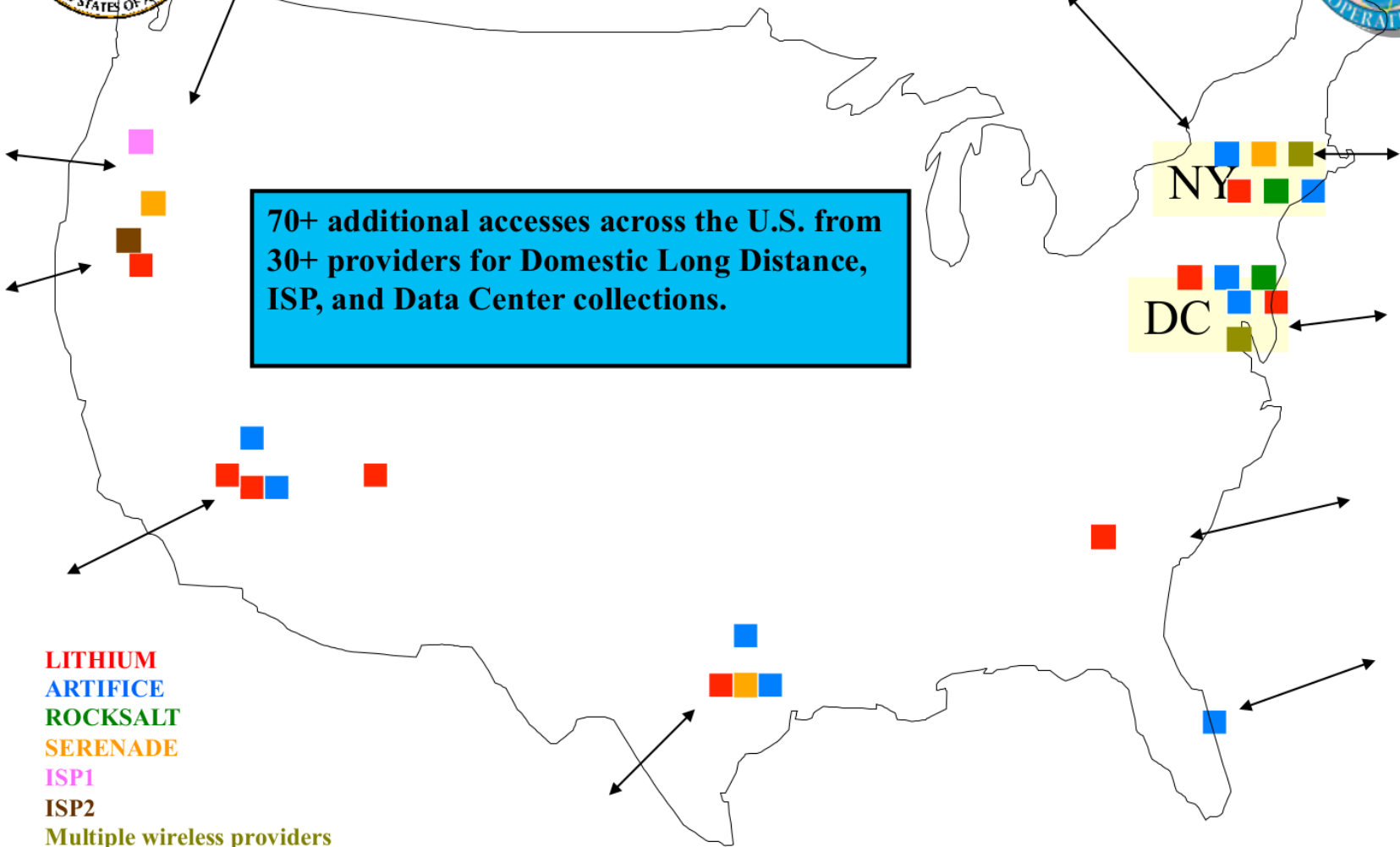


BLARNEY AT A GLANCE

Why: Started in 1978 to provide FISA authorized access to communications of foreign establishments, agents of foreign powers, and terrorists

| External Customers (Who) | Information Requirements (What) | Collection Access and Techniques (How) |
|---|-------------------------------------|--|
| Department of State | Counter Proliferation | DNI Strong Selectors |
| Central Intelligence Agency | Counter Terrorism | DNR Strong Selectors |
| United States UN Mission | Diplomatic | DNI Circuits |
| White House | Economic | DNR Circuits |
| Defense Intelligence Agency | Military | Mobile Wireless |
| National Counterterrorism Center | Political/Intention of Nations | |
| 2 nd Party-GBR, NZI, CAN, AUS | | |
| Office of Director of National Intelligence | | |
| Joint Chiefs of Staff | | |
| Department of Homeland Security | | |
| Office of Secretary of Defense | | |
| North Atlantic Treaty Organization | | |
| Military Commands (Army, EUCOM) | | |
| | Partnerships (Where) | Legal Authorities (Approvals) |
| | NSA - SSO, TAO, NTOC, CES, A&P... | NSA FISA |
| | CIA | CT FBI FISA |
| | FBI - Headquarters, NY, and DC | FISA Amendment Act (FAA) |
| | FBI - Engineering Research Facility | CI FBI FISA |
| | DOJ | BR FISA |
| | Commercial Providers | PR/TT FISA |

BLARNEY Access



70+ additional accesses across the U.S. from 30+ providers for Domestic Long Distance, ISP, and Data Center collections.

- LITHIUM
- ARTIFICE
- ROCKSALT
- SERENADE
- ISP1
- ISP2
- Multiple wireless providers

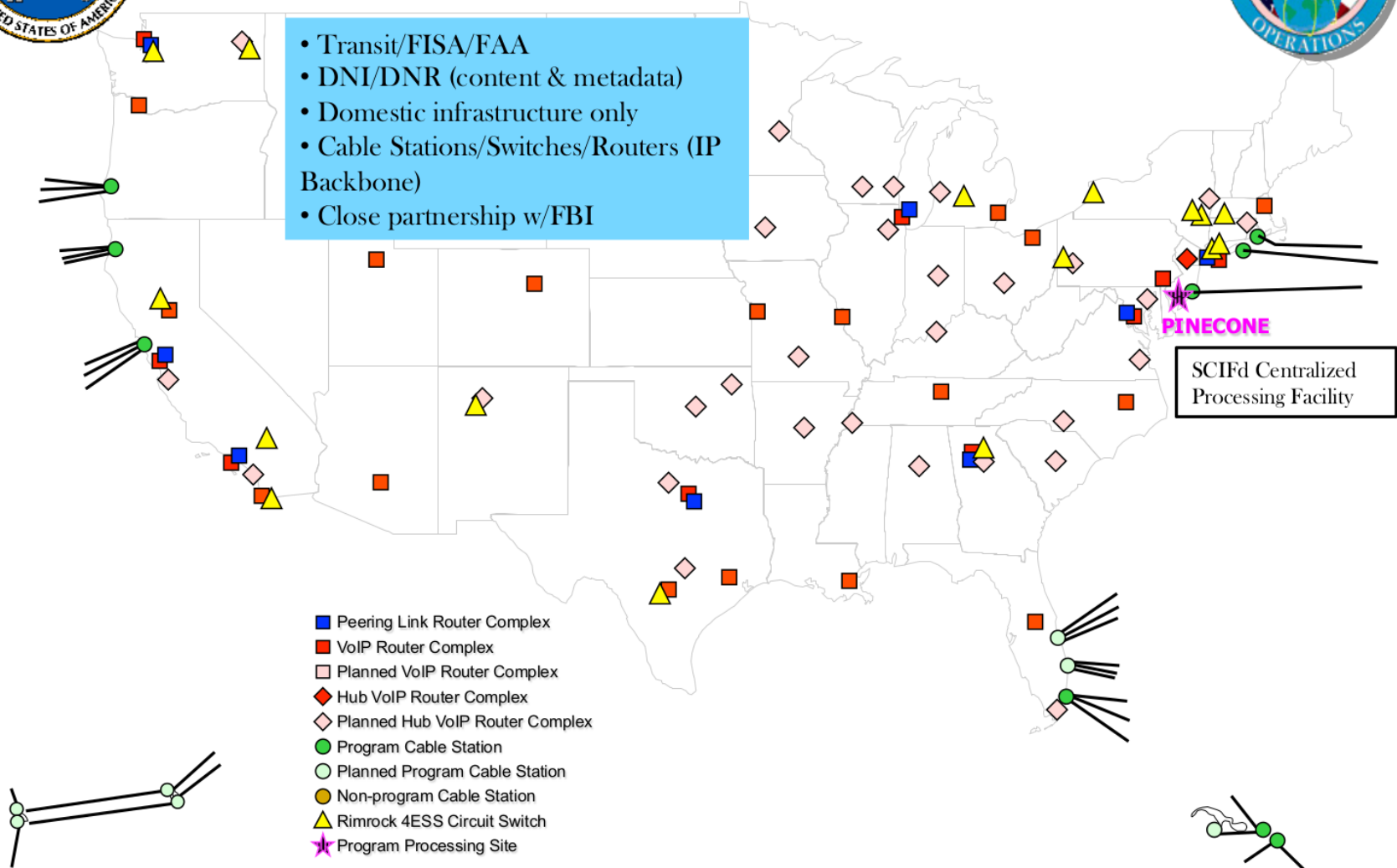


TOP SECRET // COMINT // NOFORN//20291130

FAIRVIEW At a Glance



- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Stations/Switches/Routers (IP Backbone)
- Close partnership w/FBI



TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130

STORMBREW At a Glance



Seven Access Sites – International “Choke Points”



- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Station/Switches/Routers (IP Backbone)
- Close partnership w/FBI & NCSC

TOP SECRET // COMINT // NOFORN//20291130



Corporate Funding Profile

| | <u>FY10</u> | <u>FY11</u> |
|----------------|--------------|-----------------|
| PFR: | \$187.2M | \$205.1M |
| Cyber: | \$250.9M | \$122.7M |
| FISA: | \$ 41.4M | \$ 45.9M |
| <u>*Other:</u> | <u>\$ 0M</u> | <u>\$ 10.0M</u> |
| TOTAL: | \$479.5M | \$383.7M |

* NCSC Cyber Zone 4 (OCONUS router expansion)



TOP SECRET // COMINT // NOFORN//20291130



Program Funding Break-out

| | <u>FY10</u> | <u>FY11</u> |
|-----------------|-----------------|-----------------|
| BLARNEY: | \$ 89.7M | \$ 88.0M |
| FAIRVIEW: | \$232.2M | \$188.9M |
| STORMBREW: | \$118.0M | \$ 66.8M |
| <u>OAKSTAR:</u> | <u>\$ 39.6M</u> | <u>\$ 40.0M</u> |
| TOTAL: | \$479.5M | \$383.7M |

TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130



Corporate Strategic Initiatives

- FISA Amendment Act (FAA)
- Comprehensive National Cyber Security Initiative (CNCI)
 - Expand CONUS/OCONUS Access
 - New access sites
 - Infrastructure build-out at existing access locations
 - NCC TURMOIL Deployments
- Explore & Exploit New LOB/Capabilities
 - VPNs
 - Mobility networks
 - F-F Algorithm Development (beyond Port-25)
 - Social networking
- Explore & Exploit New Partnering Relationships
 - 2 New ISPs
 - Maktoob via data centers

TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130



Comprehensive National Cyber Security (CNCS)

TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130



Corporate CNCI Funding Profile

| | <u>FY10</u> | <u>FY11</u> |
|-----------------|-----------------|-----------------|
| BLARNEY: | \$ 9.0M | \$12.1M |
| FAIRVIEW: | \$144.0M | \$73.1M |
| STORMBREW: | \$ 80.8M | \$22.9M |
| <u>OAKSTAR:</u> | <u>\$ 17.1M</u> | <u>\$14.6M</u> |
| TOTAL: | \$250.9M | \$122.7M |

TOP SECRET // COMINT // NOFORN//20291130



FY10/FY11 CNCI Expansion

- New Access Sites
 - FY10 – 5 new access locations (4 cable, 2 router)
 - FY11 – 5 new access locations (1 cable, 4 router)
- Infrastructure Build-outs/Existing Access Expansion
 - FY10 anticipated – ingest **530 Gbps** of data
 - FY11 anticipated – ingest **760 Gbps** of data
- TURMOIL Processing Suites (Tech Insertion)
 - FY10 = 0
 - FY11 = 44
 - TOTAL = 44***
 - *Original request 55*
 - } **Sliding schedule**



TOP SECRET // COMINT // NOFORN//20291130



CNCI Challenges

- Legal Framework
 - SIGINT
 - Transit (limited value – attacks aimed at the U.S.)
 - FAA (maximum value – Cyber cert; initial value – tie signatures to existing Certs)
 - Defense (.mil, .gov, .dib)
- UTT tasking/targeting tool (ability to task signatures)
- Data repositories
- Analytical support
- TURMOIL defense s/w applications

TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130



Corporate FAA Reporting Metrics

TOP SECRET // COMINT // NOFORN//20291130

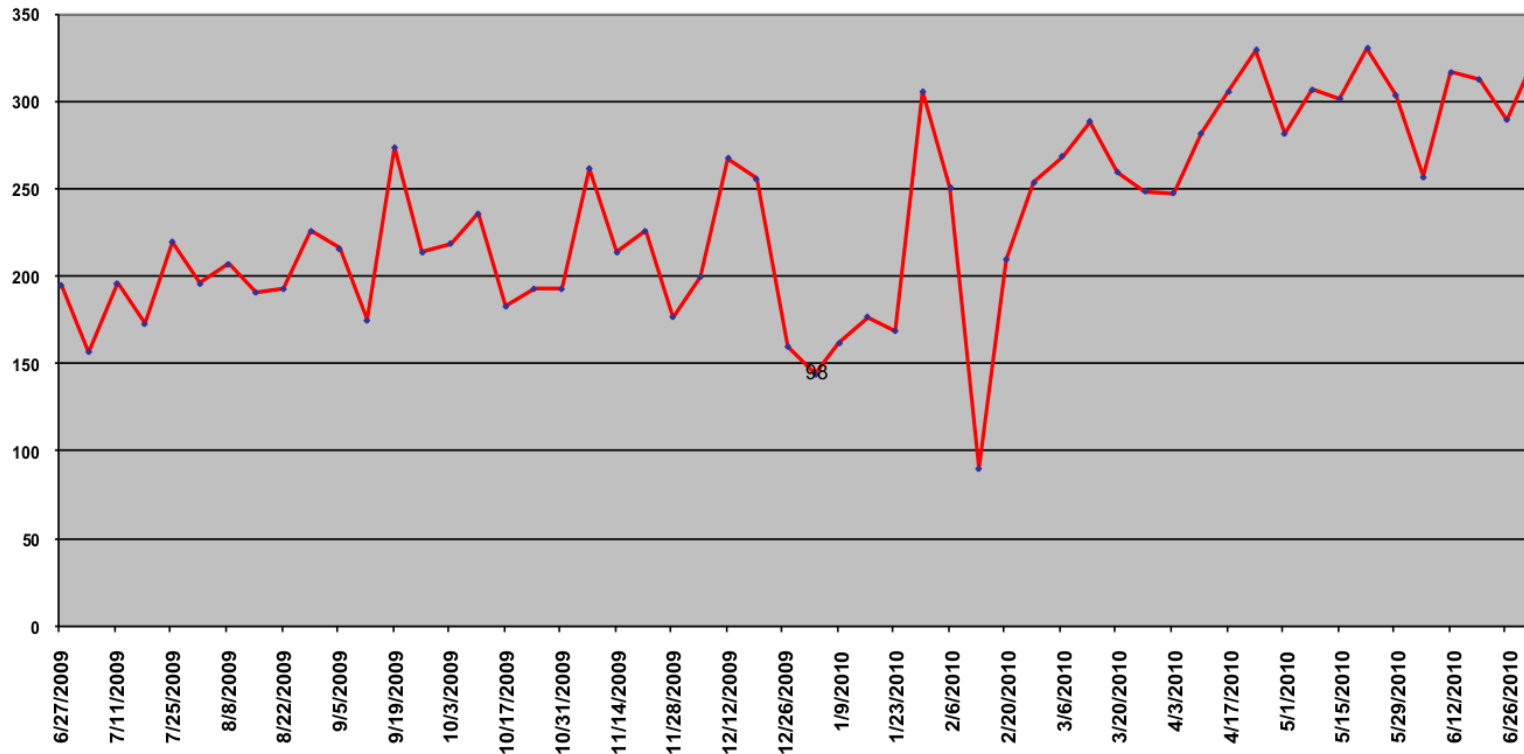


TOP SECRET // COMINT // NOFORN//20291130



Corporate FAA Reporting Metrics

FAA REPORTS -
Weekly Stats thru 3 July 10



TOP SECRET // COMINT // NOFORN//20291130

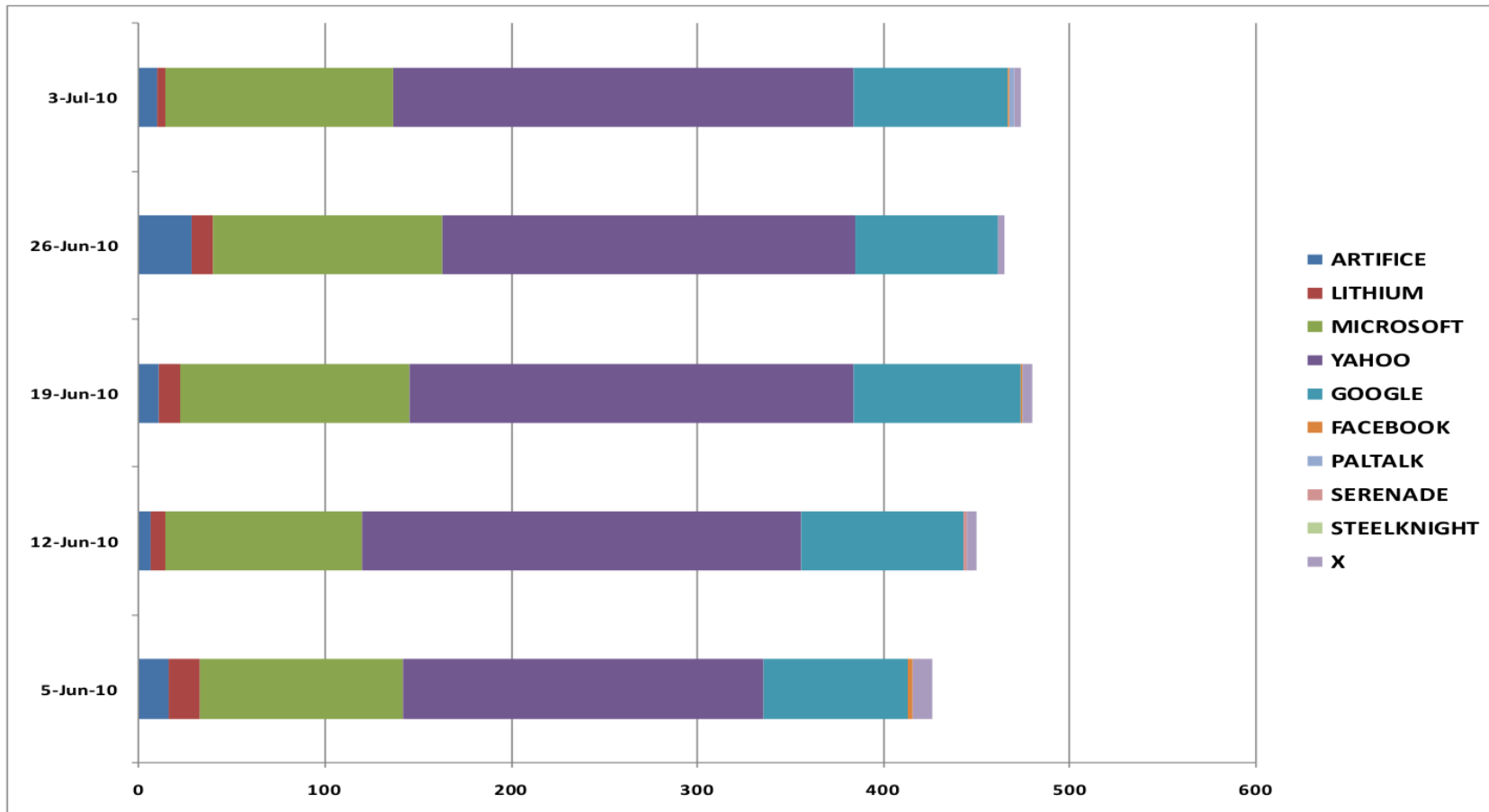


TOP SECRET // COMINT // NOFORN//20291130



Corporate FAA Reporting Metrics

FAA Reports by Provider



TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130

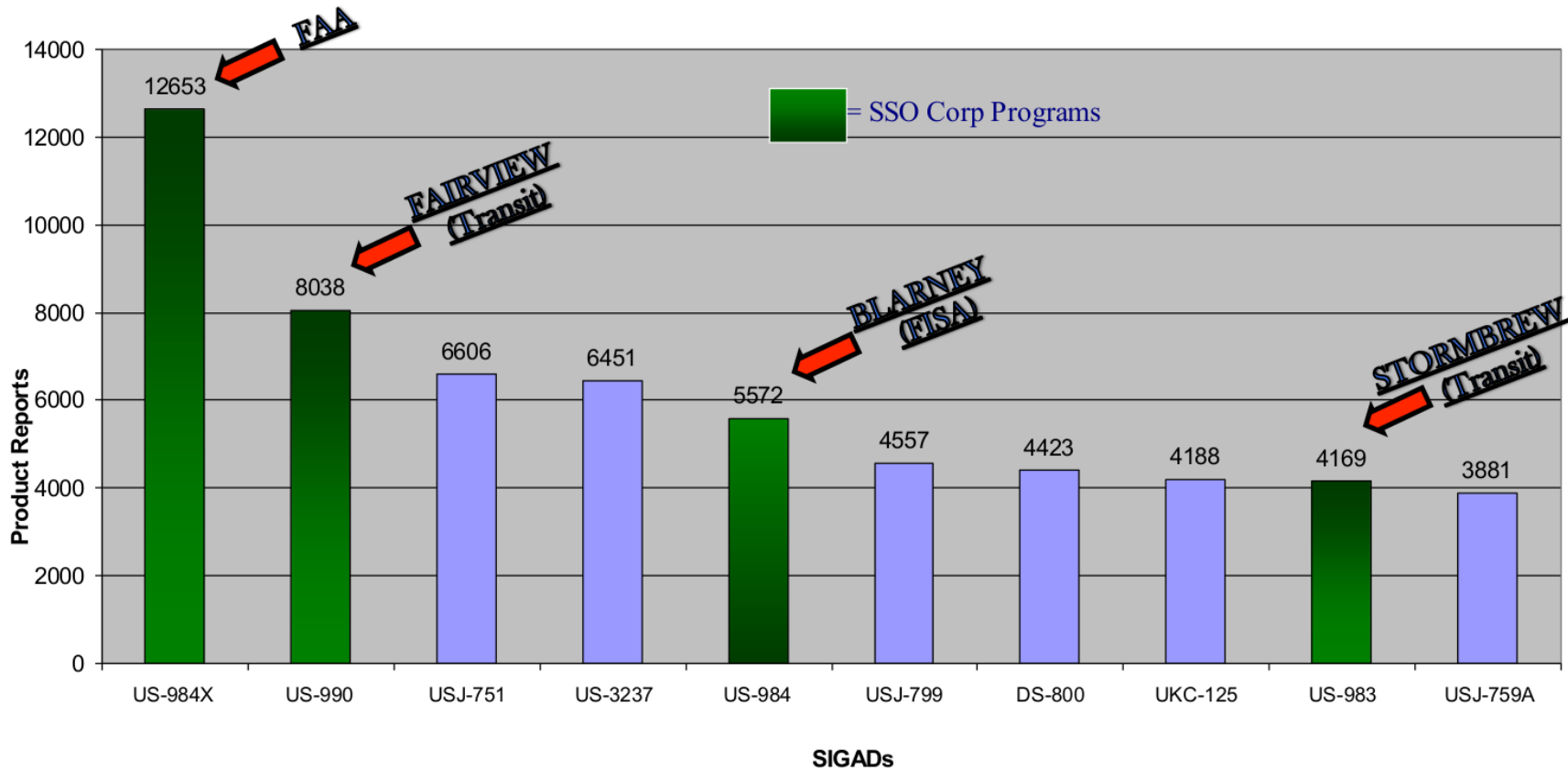


Corporate Transit Reporting Metrics & Highlights

TOP SECRET // COMINT // NOFORN//20291130



Top Ten SIGADs for 2009 July 2009 – June 2010





TOP SECRET//SI//OC//NOFORN

FAIRVIEW

SSO FAIRVIEW Overview

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

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

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

FAIRVIEW

International Cables

(TS//SI//NF)



(TS//SI//NF)

TOP SECRET//SI//OC//NOFORN

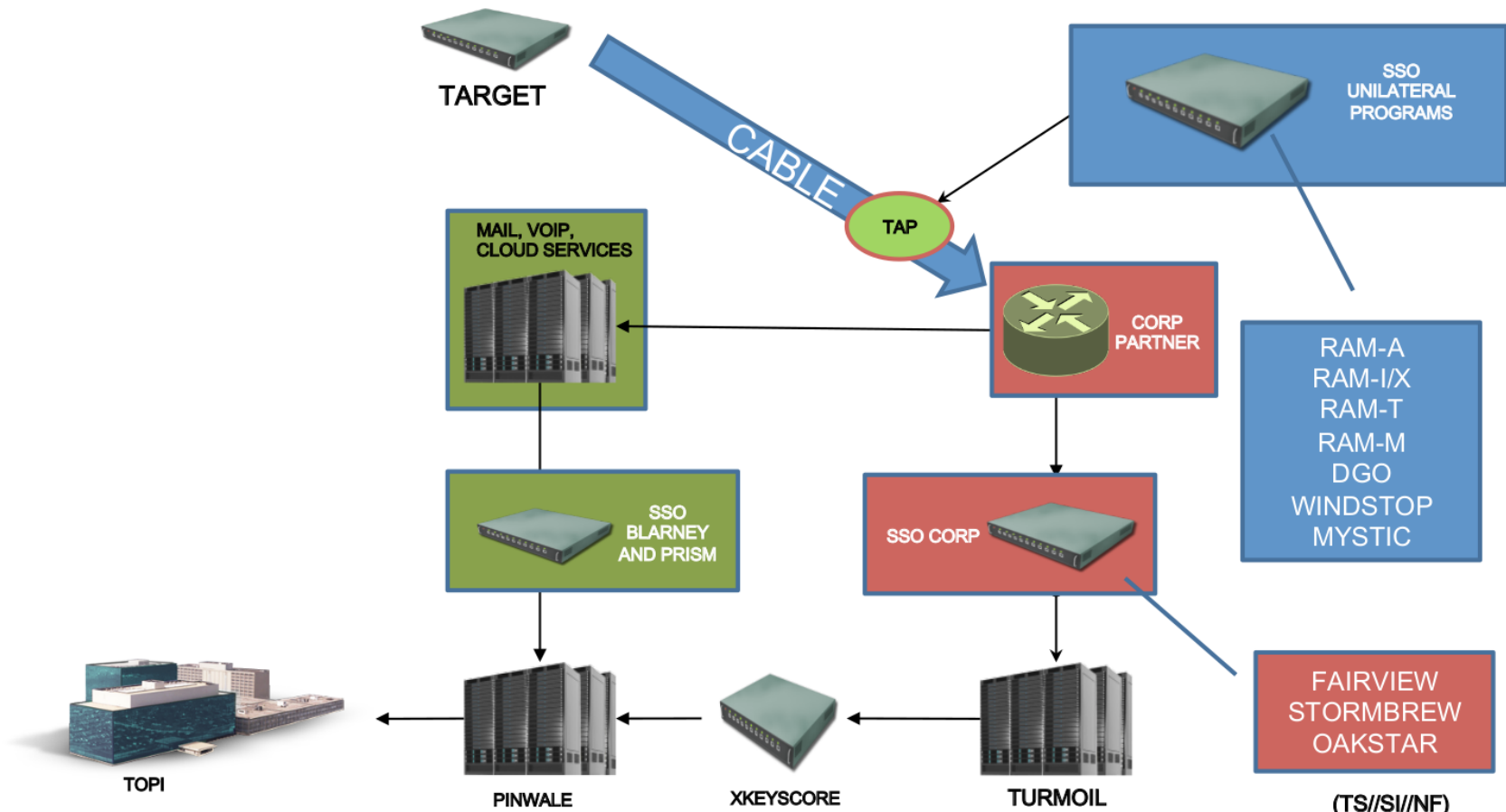


TOP SECRET//SI//OC//NOFORN



WHERE SSO IS ACCESSING YOUR TARGET

(TS//SI//NF)



TOP SECRET//SI//OC//NOFORN

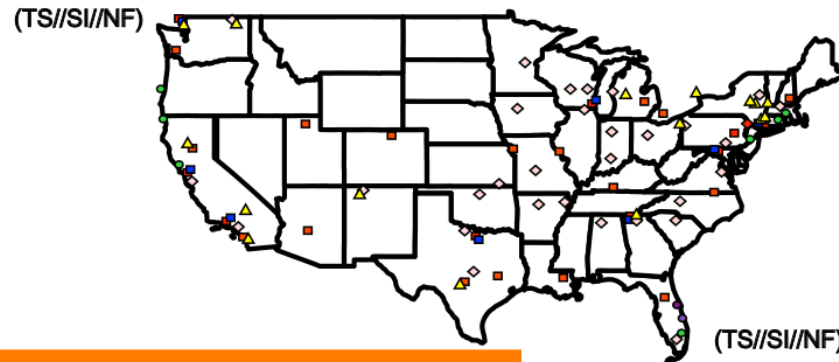


TOP SECRET//SI//OC//NOFORN

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



TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

FAIRVIEW

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

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

FAIRVIEW

Transit Authority

(TS//SI//NF)



(TS//SI//NF)

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

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.

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

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

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

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.

TOP SECRET//SI//OC//NOFORN



TOP SECRET//SI//OC//NOFORN

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.

TOP SECRET//SI//OC//NOFORN



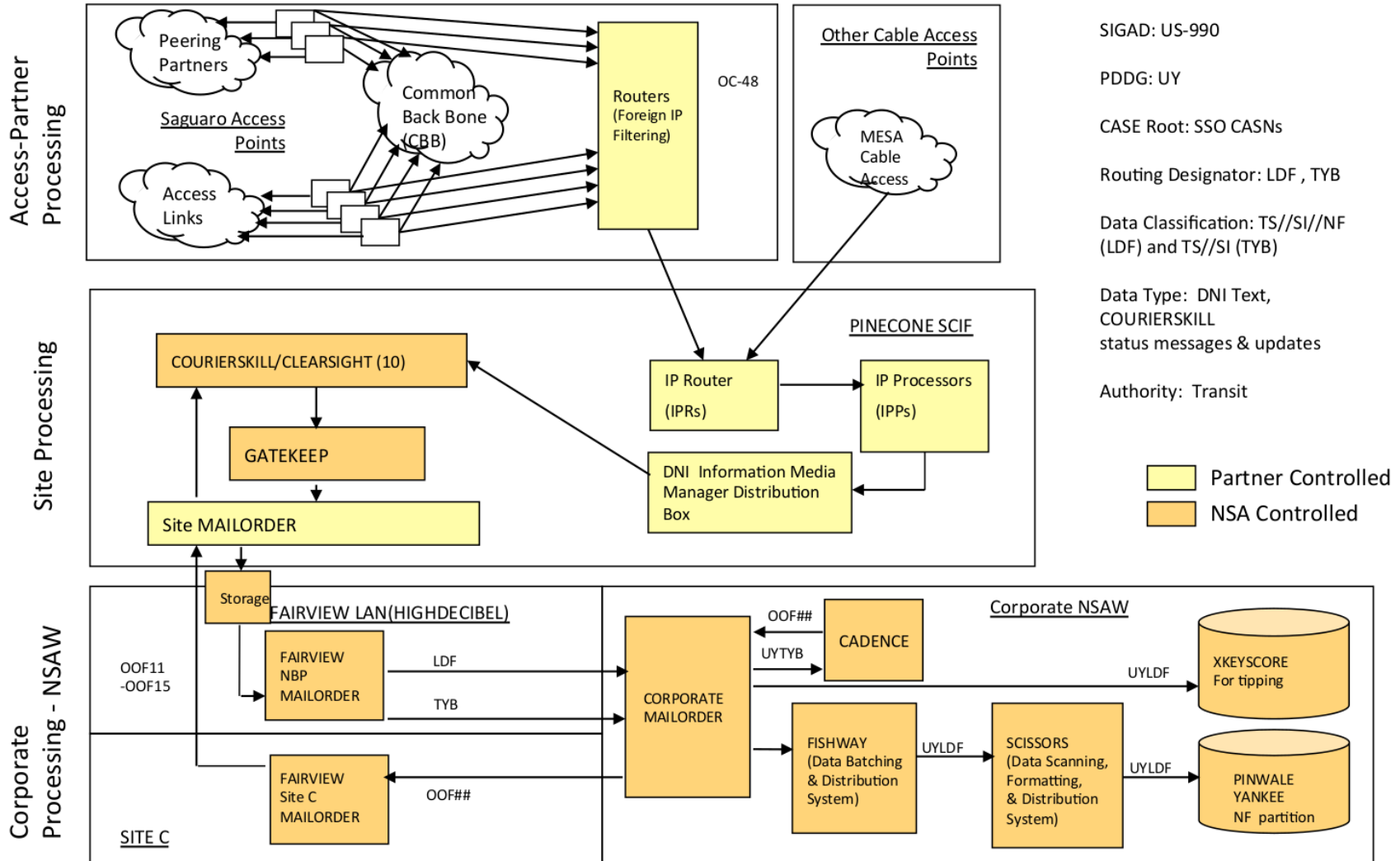
Dataflow Diagrams

April 2012

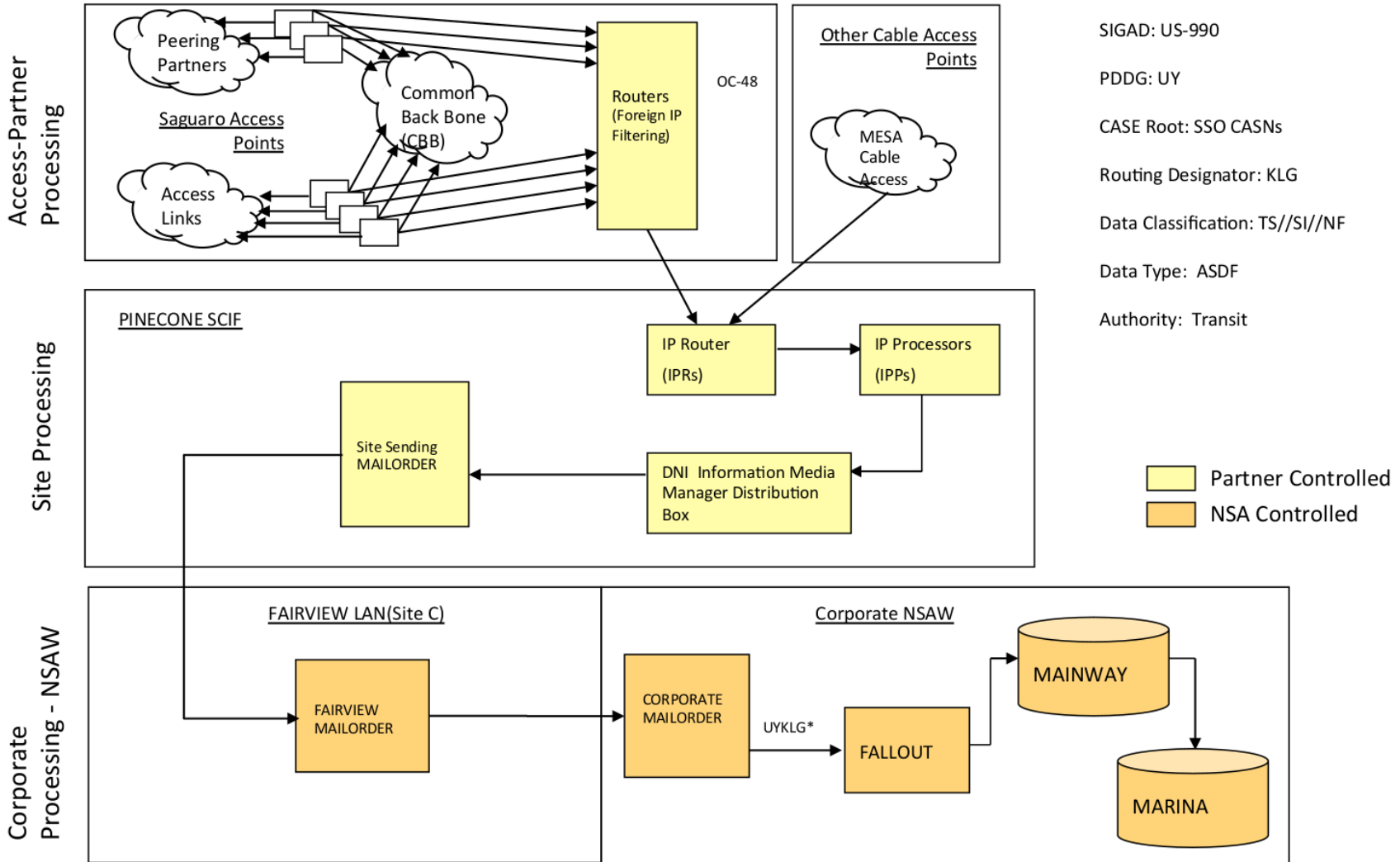
Note: Please refer to previous diagrams for decommissioned systems.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20361101

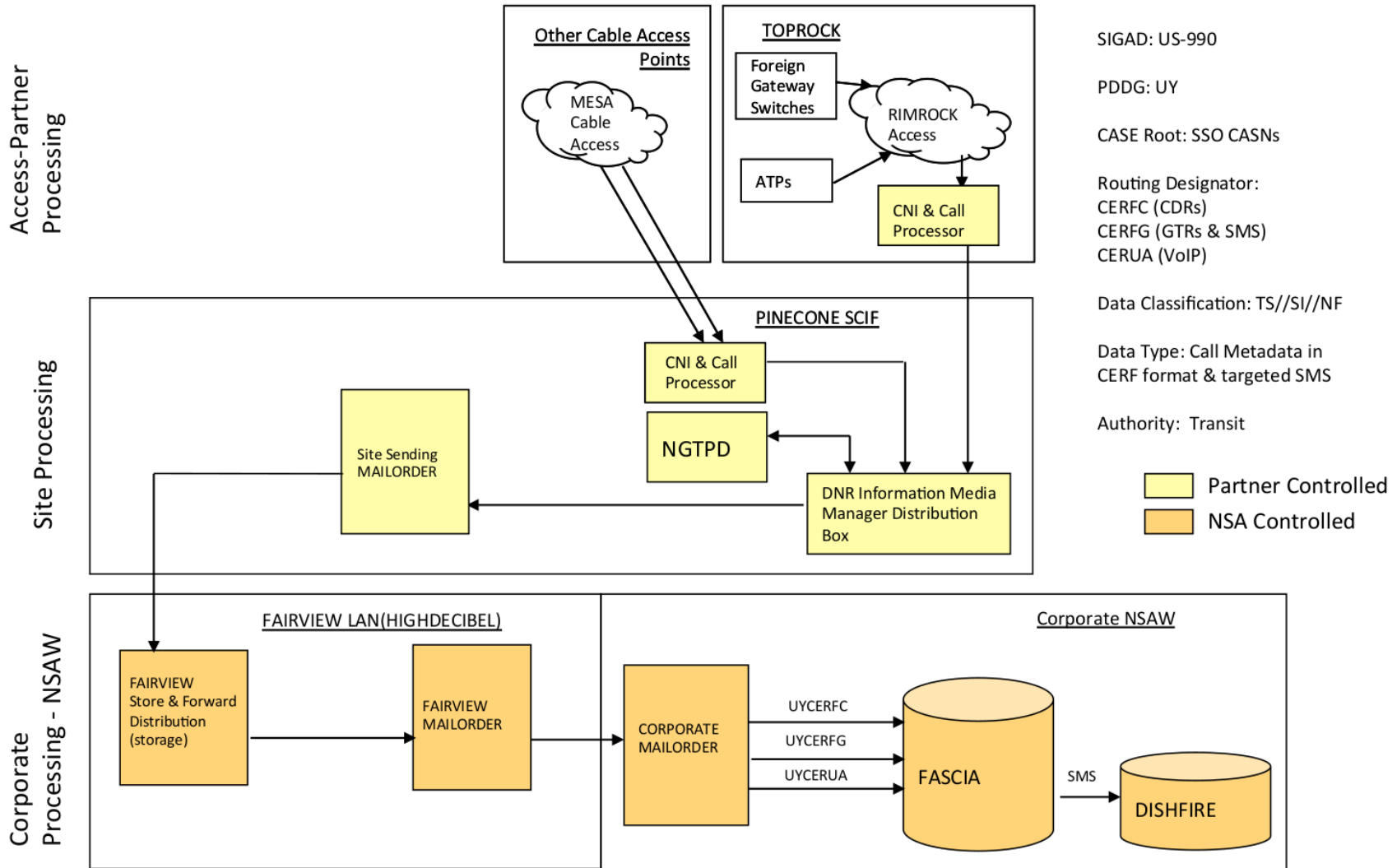
Transit DNI Content (BUGCATCHER)



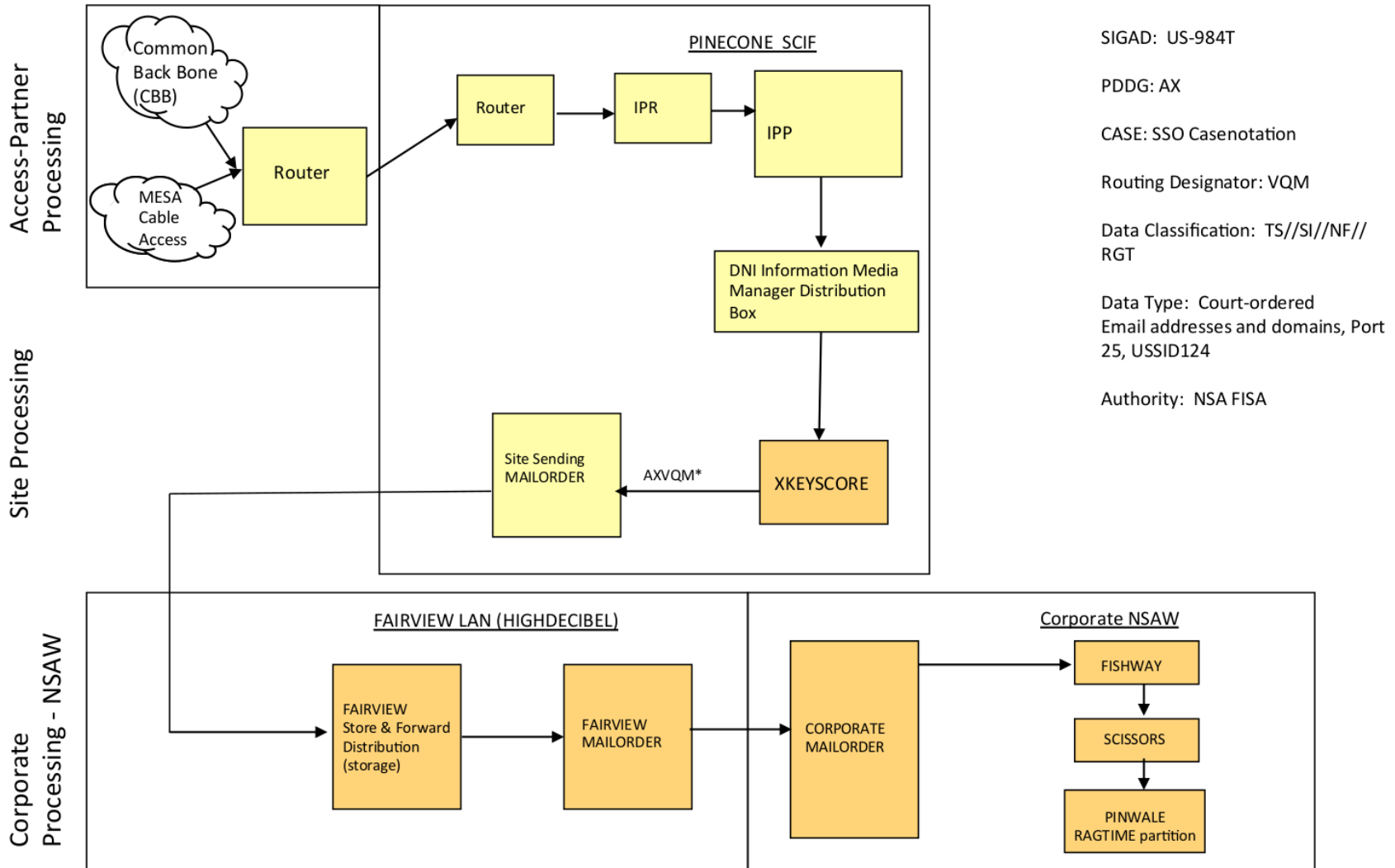
Transit DNI Metadata (IMDRs)



Transit DNR Metadata & SMS



FAIRVIEW NSA FISA Email



SIGAD: US-984T

PDDG: AX

CASE: SSO Casenotation

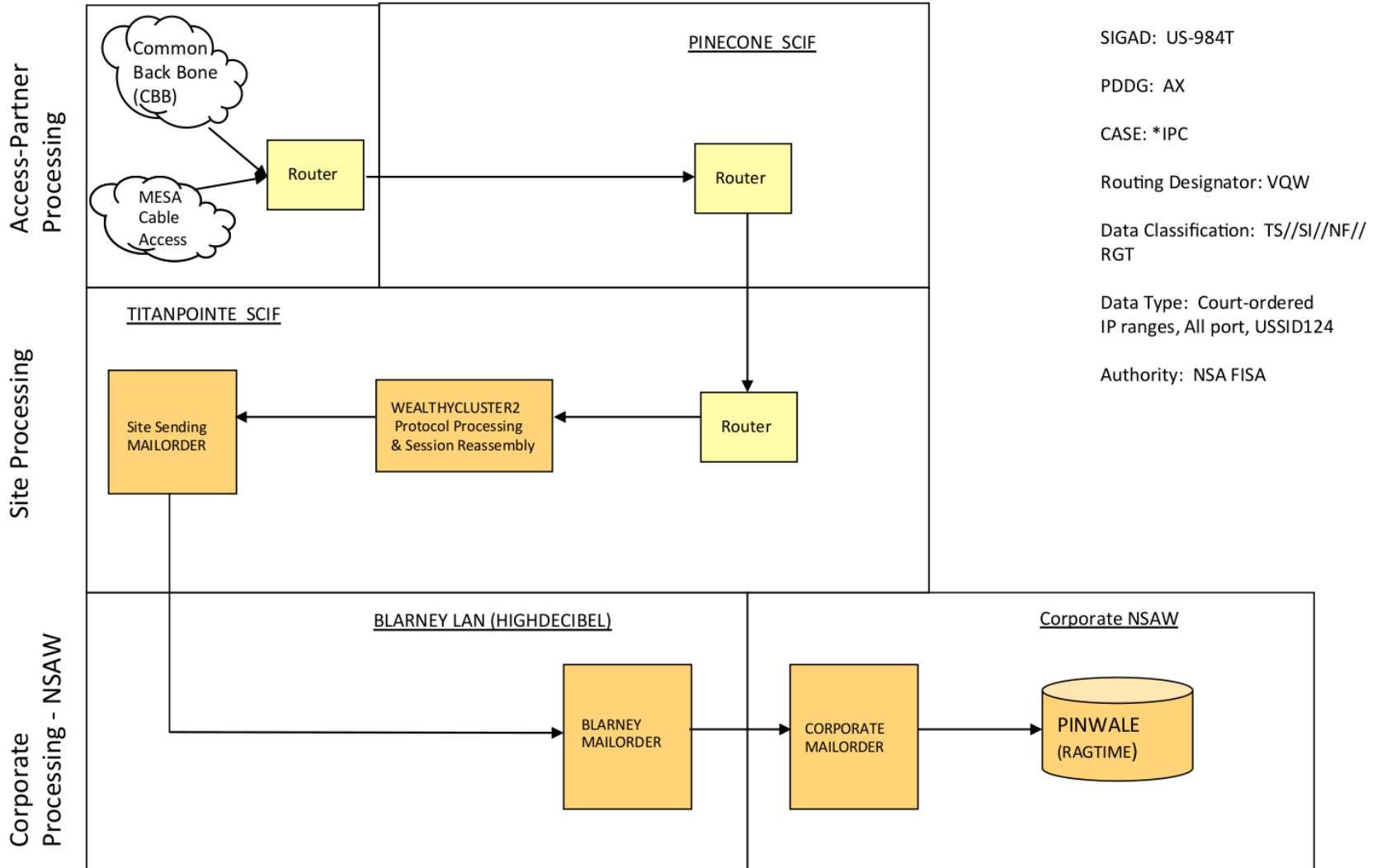
Routing Designator: VQM

Data Classification: TS//SI//NF//RGT

Data Type: Court-ordered
Email addresses and domains, Port 25, USSID124

Authority: NSA FISA

FAIRVIEW NSA FISA IP





TOP SECRET//COMINT//NOFORN

Special Source Collection

March 2013

*Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 2030108*

TOP SECRET//COMINT//NOFORN



TOP SECRET//SI//REL USA, FVEY



Cyber Threats and Special Source Operations A Current Perspective for NTOC



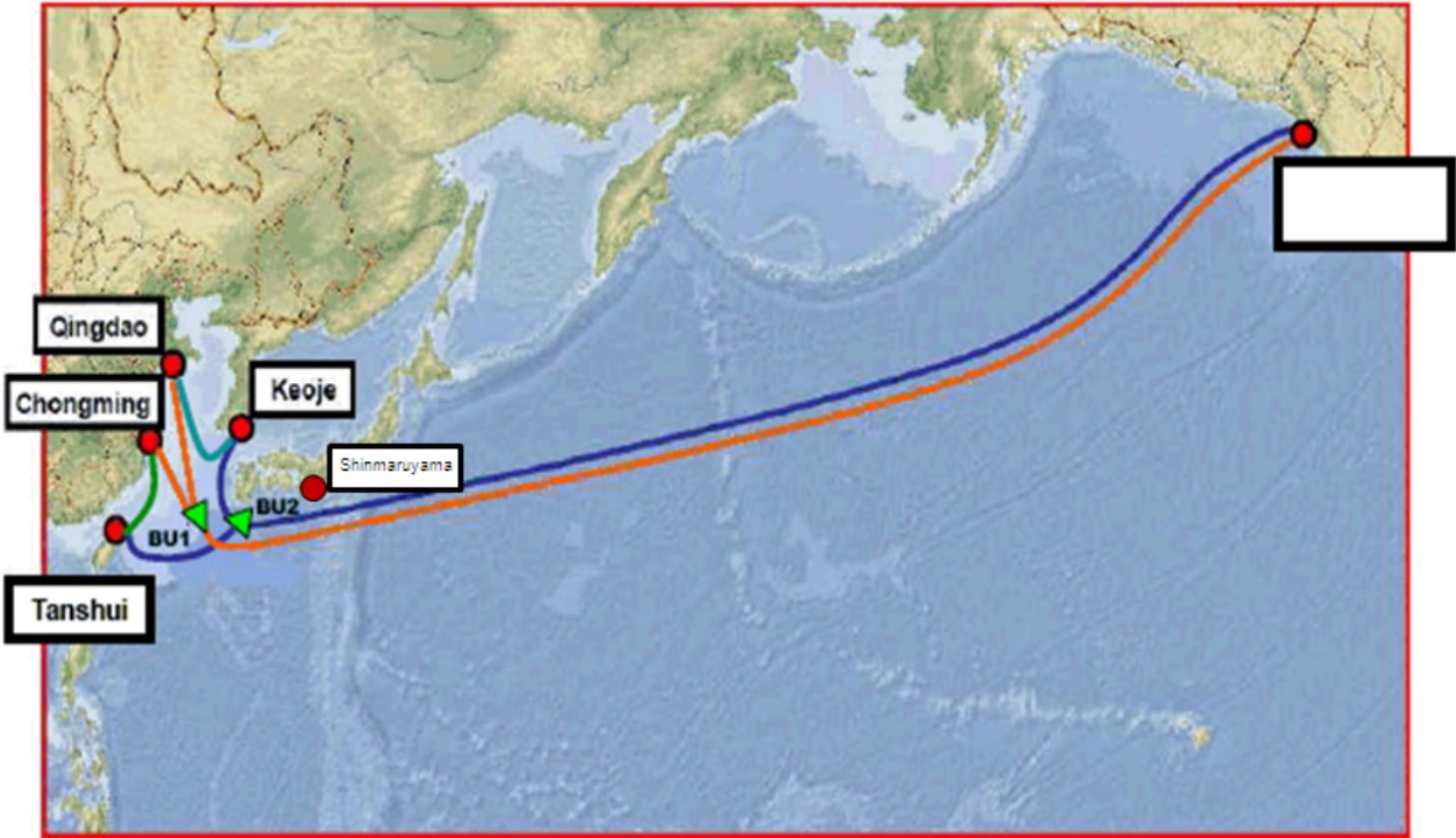
March 22, 2013

*Classified By: [REDACTED]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380301*

TOP SECRET//SI//REL USA, FVEY



**STORMBREW's BRECKENRIDGE Site was
100% Subsidized with CNCI Funding**



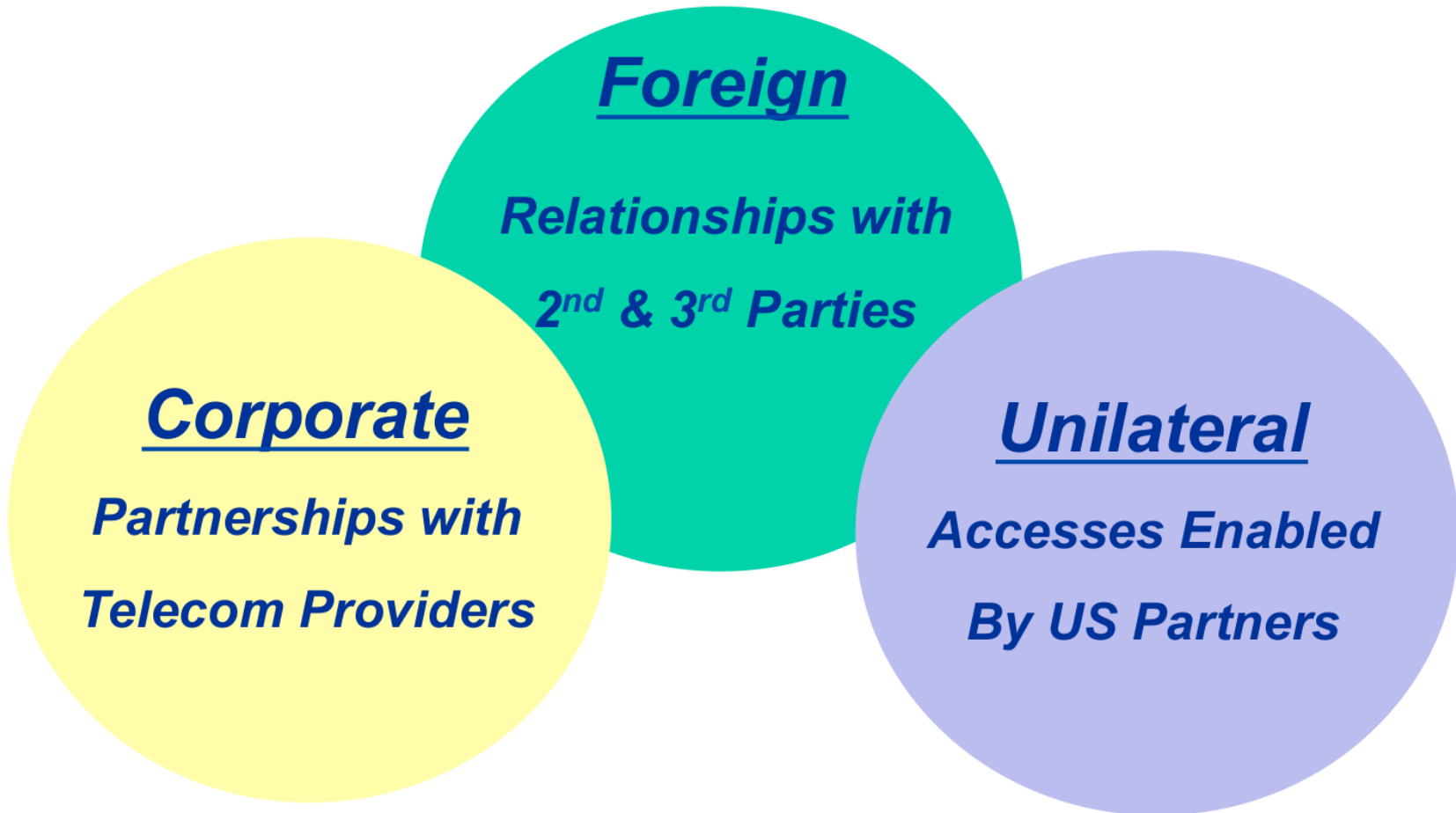


Why SSO?

- *SSO is “Big Data”*
 - *~60% of content*
 - *~75% of metadata*
- *We’re different*
 - *Nuances of individual programs*
- *Tremendous potential*
 - *Need NTOC to guide SSO*

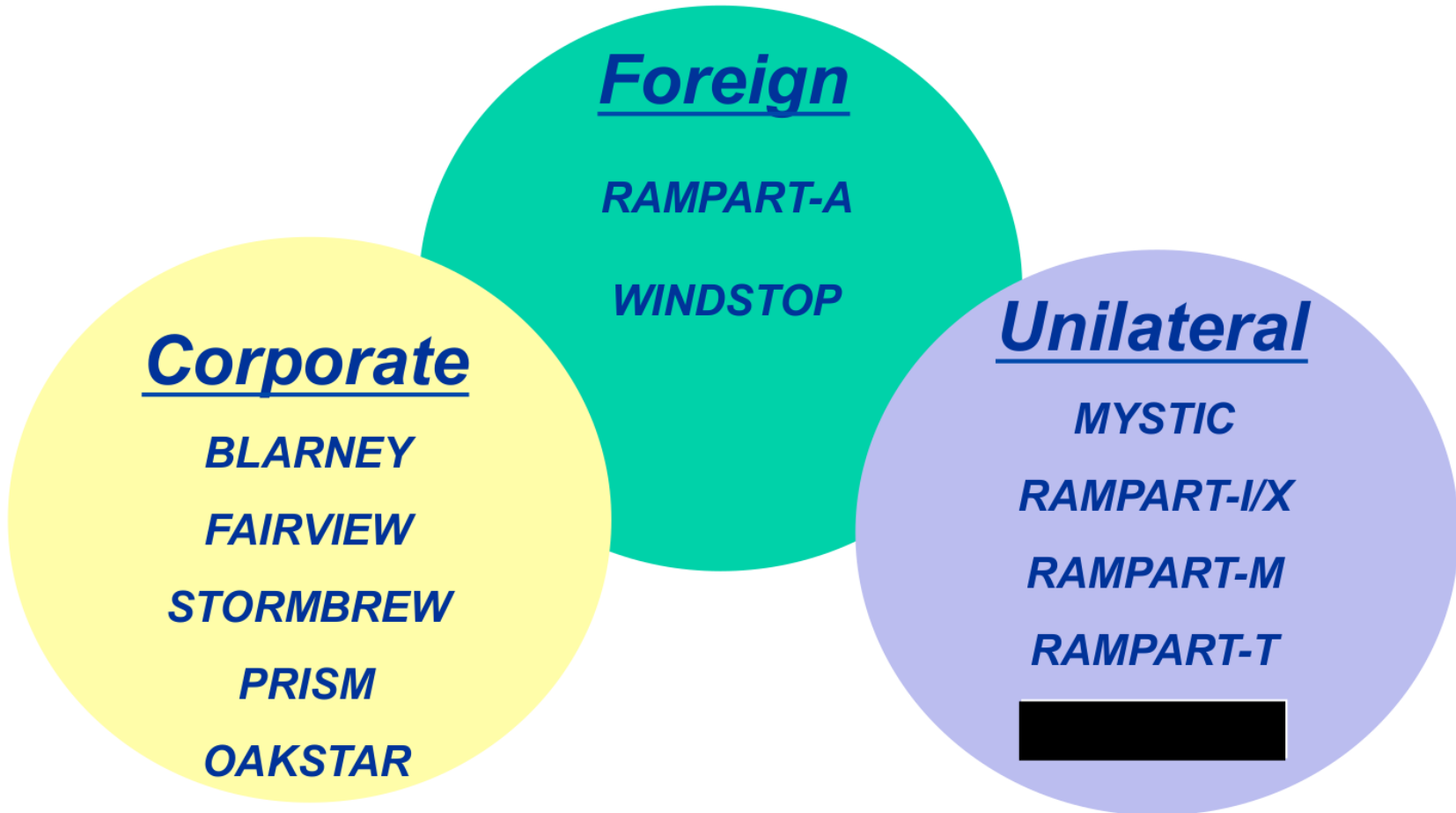


SSO Access Portfolios





SSO Access Portfolios



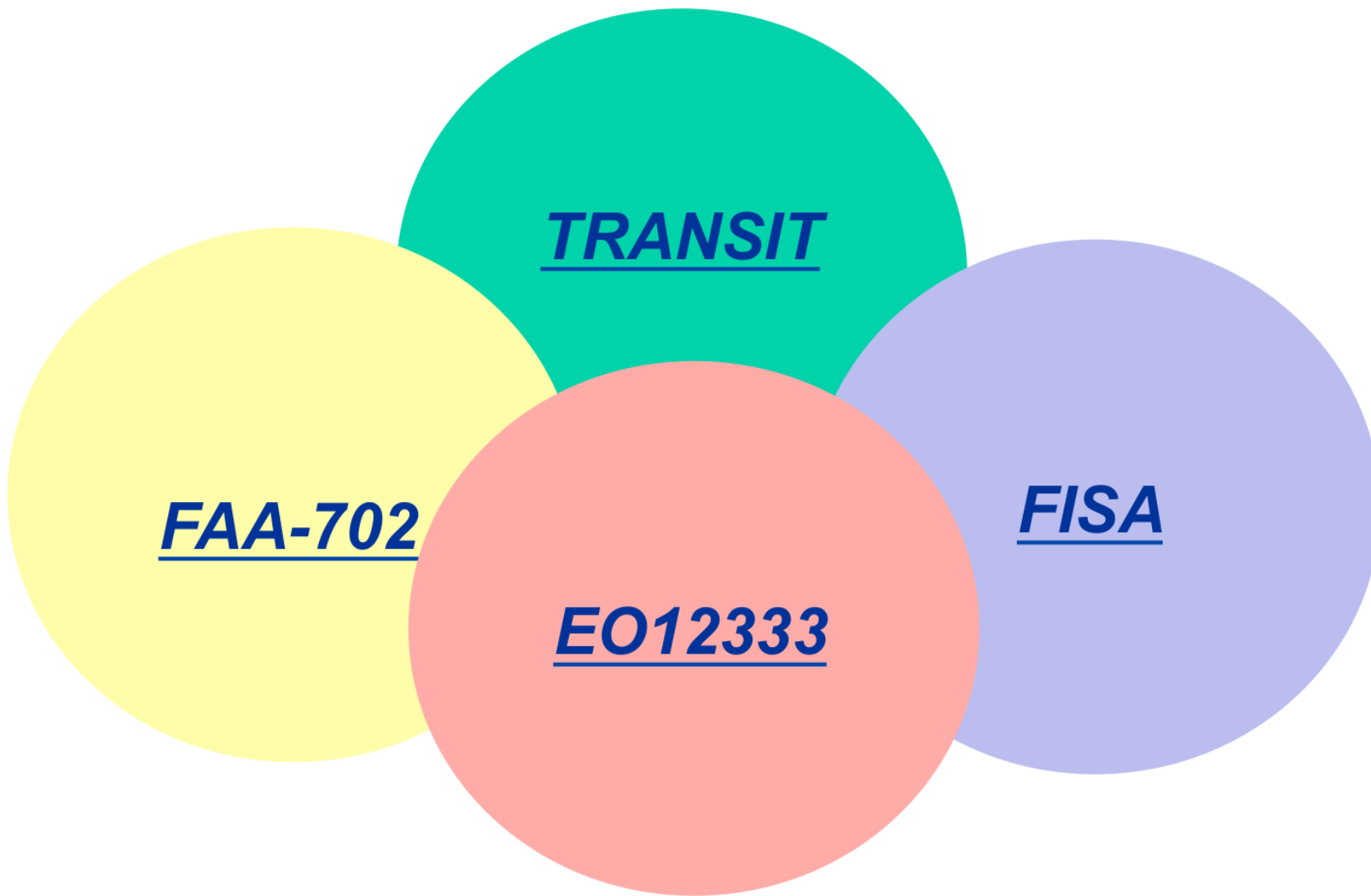


Partner Constraints

- Foreign
 - All Targeting/Signatures exposed to 2P/3P partner for approval
 - Partner approves new capabilities
- Corporate
 - FISA, FAA, TRANSIT authorities
 - *Requires FISC/DoJ permission for capabilities*
 - Partner approvals for capabilities (in some cases)
- Unilateral
 - Power/Space/Cooling at site
 - Bandwidth for data forwarding
 - Risk of site compromise

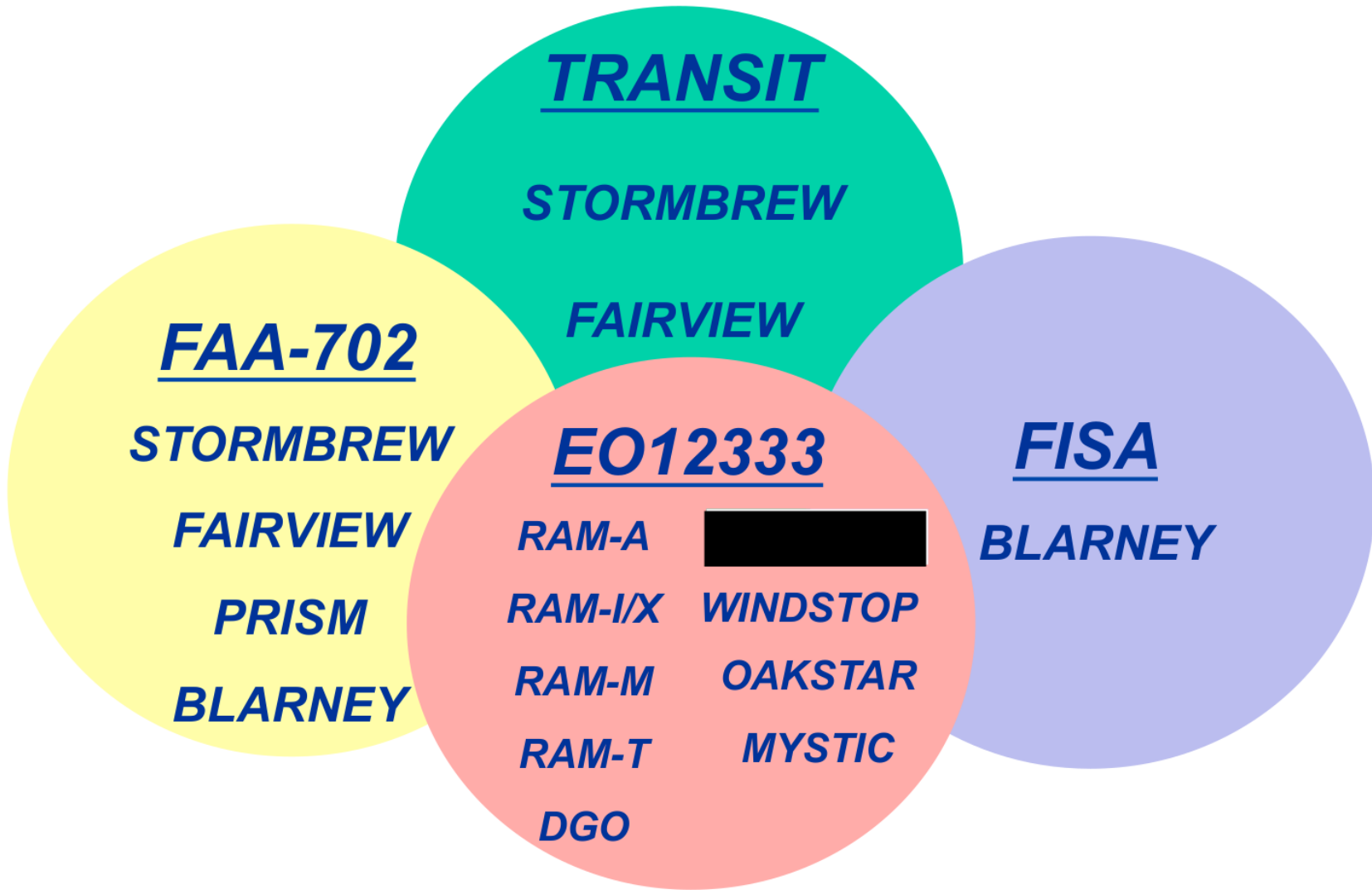


Authorities





Authorities



UNCLASSIFIED//FOR OFFICIAL USE ONLY



14 MARCH 2013

**Special
Source
Operations
Weekly**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY



(U) CORPORATE TEAM

(U//FOUO) BRIEFER: [REDACTED]



UNCLASSIFIED//FOR OFFICIAL USE ONLY

TOP SECRET//SI//NOFORN



(U) Operational Highlight

(TS//SI//NF) STORMBREW –TRANSIT DNI Metadata Collection

- **(TS//NF) Activated on 11 March at BRECKENRIDGE**
- **(U//FOUO) Metadata collection is SMTP only at this time**
- **(TS//NF) Foreignness is confirmed with IPP from FAIRVIEW**
- **(C//REL to USA, FVEY) Data is flowing into MARINA**
- **(U//FOUO) Content collection should happen soon**

**UPDATE: As of 1826Z on 13 March 2013,
STORMBREW began content collection
of SMTP under Transit Authority!!**

TOP SECRET//SI//NOFORN

LITHIUM (TS//SI//NF) BLARNEY's covername for one of their corporate partners. Need WPG ECI for company name

-

NODDY-3 (TS//SI//NF) FAIRVIEW'S covername for Coverage of Current and Forecasted NRTM Circuits. The FAIRVIEW program is acquiring DNI access (SAGUARO) from the Partner's DNI backbone which includes OC-192 and 10GE peering circuits. The Partner has provided a current view of the forecasted and equipped 10GE and OC-192 peering circuits at the eight SNRCs as of March 2009. Based on the information presented, by the end of 2009, the total number of forecasted 10GE peering circuits at the SNRCs will be approximately six times greater than OC-192 peering circuits. However, the growth in 10GE circuits in 2009 is about 19 times greater than the forecasted growth for OC-192 circuits. As these additional links become active it is imperative that FAIRVIEW have the ability and the agility to follow SIGINT targets of interest. This action will provide 100% coverage of the 2009 forecasted 10GE and OC-192 links. This broad coverage approach is a key part of a larger effort to recast the FAIRVIEW DNI router access to be more agile and more high-value intelligence focused as part of the program's effort to provide broad access, continuous survey and focused collection.

-

SAGURA (TS//SI//NF) DNI access from FAIRVIEW'S Partner's DNI backbone which includes OC-192 and 10GE peering circuits. The Partner has provided a current view of the forecasted and equipped 10GE and OC-192 peering circuits at the eight SNRCs as of March 2009. Based on the information presented, by the end of 2009, the total number of forecasted 10GE peering circuits at the SNRCs will be approximately six times greater than OC-192 peering circuits. However, the growth in 10GE circuits in 2009 is about 19 times greater than the forecasted growth for OC-192 circuits. As these additional links become active it is imperative that FAIRVIEW have the ability and the agility to follow SIGINT targets of interest. This action will provide 100% coverage of the 2009 forecasted 10GE and OC-192 links. This broad coverage approach is a key part of a larger effort to recast the FAIRVIEW DNI router access to be more agile and more high-value intelligence focused as part of the program's effort to provide broad access, continuous survey and focused collection.

-

SLIVER (TS//SI//NF) SLIVER is a proof-of-concept (POC) is an effort to enable cross-mission (CNO) collaborative capabilities in a global setting. Under the SLIVER initiative, passive IP sensor nodes will be deployed at two CONUS sites and two OCONUS sites. These nodes will be fed by a small amount of traffic volume. The CONUS nodes will support both Lithium commercial network security functions, as well as SIGINT and SIGINT-enabled CND applications

(i.e., end-point characterization data and IP flow data). Within the SLIVER timeframe, due to OPSEC constraints, the OCONUS nodes will only be configured to support Lithium commercial network security functions -- any Lithium-derived metadata from the OCONUS nodes will be sent to FAIRVIEW's centralized processing facility (PINECONE), under applicable SIGINT authority, for analysis and exploitation. In addition to these passive sensor nodes, active commercial security nodes will also be deployed at both the CONUS and OCONUS sites and used commercially in order to provide essential mission cover.

-

SORA-2

(TS//SI//NF) IP Access Expansion effort for FAIRVIEW. One of the areas of FAIRVIEW's DNI backbone access (Saguaro) that has not yet been sufficiently exploited is the access side of the Common Backbone (CBB) network. The major reason for this is the sheer number of access links - tens of thousands - which would make 100% coverage prohibitively expensive. One way to overcome this constraint is to monitor uplinks out of the access routers toward CBB backbone or aggregation routers. Even so, the number of uplinks is still numerous, requiring an additional selection/prioritization strategy. Lithium, in concert with ODD, developed a strategy that rank orders access routers using several different metrics, such as the following: PRI Value, Country Value, PAA Value, CD Value and CCCD Value. The top eight router uplinks, as outlined in the attached proposal, have been analyzed and deemed of high SIGINT interest. Therefore, we are requesting approval to deploy monitoring on these uplinks.

DYNAMIC PAGE -- HIGHEST
POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO
USA AUS CAN GBR NZL

(S//SI) FAIRVIEW and STORMBREW: 'Live' - On the Net

FROM: [REDACTED] and [REDACTED]
Special Source Operations (S332)
Run Date: 11/19/2003

(TS//SI) Two special source collection programs - S332's FAIRVIEW and STORMBREW - are producing SIGINT successes by "living on the global intelligent network." In September of this year, FAIRVIEW quietly turned on a new DNI (Digital Network Intelligence) collection capability that quickly proved a valuable source of intelligence: A&P's Office of Proliferation and Arms Control (S2G21) issued the first SIGINT product report sourced from this new access on September 24. Then, less than a month later, the first E-series product report (extremely sensitive serialized reports sent to a limited audience) was issued by International Security Issues, (S2C21). Many other offices now use this collection, as well - the FAIRVIEW DNI access is extremely high-volume and delivers a very broad target set covering all SIGINT product lines. For example, the initial deployment of the FAIRVIEW DNI access, for e-mail only, is now forwarding more than one million emails a day to the keyword selection system at NSAW.

(TS//SI) STORMBREW has a complementary large-scale DNI collection effort (covername PERFECTSTORM) that is just about ready for prime time. As the large-scale effort was being developed, STORMBREW deployed several QRC (Quick Reaction Capability) collection systems that have yielded critical intelligence supporting the Global War on Terrorism. STORMBREW engineers then worked with FAIRVIEW engineers to transfer this collection architecture to FAIRVIEW. Recently, FAIRVIEW identified the "other side" of one of the STORMBREW QRC links, and was able to use the same collection architecture to rapidly put this new link on cover. This type of complementary access provides the A&P analysts with more complete coverage of their target. In addition, STORMBREW and FAIRVIEW personnel worked side-by-side with CES personnel to add Voice over IP processing capabilities to both of these accesses to further exploit the targets' communications.

(TS//SI) In addition to email, FAIRVIEW and STORMBREW are also collecting metadata, or data about the network and the communications it carries. For September 2003 alone, FAIRVIEW captured several trillion metadata records - of which more than 400 billion were selected for downstream processing or storage. This metadata will be used to enable the surgical collection of much smaller amounts of target-rich data - which should extend beyond FAIRVIEW and STORMBREW to many other DNI accesses across NSA. This metadata is flowing to MAINWAY (contact chaining

database) today, and a major interface to the Knowledge System Prototype (KSP) is only days away from its operational debut. Both the STORMBREW and FAIRVIEW teams are working closely with the Network Analysis Center, the Collection Strategies and Requirements Center, and analysts throughout A&P to foster metadata exploitation, focus the access, improve the selectors and filters, and hunt for targets within the access. This collaborative process is the foundation for SIGINT success on the Net.

(TS//SI) FAIRVIEW and STORMBREW also provide other major international accesses that support all A&P SIGINT product lines. In a recent complementary modernization effort, the FAIRVIEW and STORMBREW programs quadrupled SIGINT production from these circuit-switched accesses, only a few months after implementation. As the FAIRVIEW and STORMBREW programs continue to expand their "live" presence on the global net, we are expecting even greater insight into the net itself, and the communications of our targets, resulting in similar SIGINT production gains from these packet-switched accesses.

[Comments/Suggestions about this article?](#)

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121

Information Own [REDACTED] S012 [REDACTED]
Page Publisher: [REDACTED], S0121, [REDACTED]
Last Modified: 11/09/2012 / Last Reviewed: 11/09/2012

DYNAMIC PAGE -- HIGHEST POSSIBLE
CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR
NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007
DECLASSIFY ON: 20320108

(TS//SI) BRECKENRIDGE for STORMBREW Collection
By [REDACTED] on 2009-10-28 1035

7 October 2009

(TS//SI//NF) STORMBREW has completed SCIF construction and also received security certification for BRECKENRIDGE, its latest collection site on 11 September 2009. The 10,000 square foot facility is equipped with the necessary power, communications and equipment racks to support the planned near-term deployment of 15 TURMOIL systems, providing 150G of processing against the newly acquired [REDACTED]. The results of a recent signal survey, conducted by SSO, indicates a potentially rich target environment of both DNI and DNR. Initial collection system deployments are scheduled for 2nd quarter 2010. The BRECKENRIDGE/[REDACTED] effort commenced in February 2007 and is the first "cable-head" collection effort conducted under STORMBREW.

(U//FOUO) POC: [REDACTED], Deputy PD STORMBREW, [REDACTED].

(TS//SI//NF) FAIRVIEW: CLIFFSIDE Site - Collection Resumes After ~5 Months

By [REDACTED] on 2011-08-23 0805

(TS//SI//NF) On 5 Aug 2011, collection of DNR and DNI traffic at the FAIRVIEW CLIFFSIDE trans-pacific cable site resumed, after being down for approximately five months. Collection operations at CLIFFSIDE had been down since 11 March 2011, due to the cable damage as a result of the earthquake off of the coast of Japan. The initial damage assessment showed the loss of collection of 275 E1 DNR circuits and 55 DNI circuits. Since the cable was repaired and returned to service (5 Aug), FAIRVIEW operations has tasked 205 E1 DNR circuits and 37 DNI circuits for collection. Environmental survey continues to compare the old environment footprint to the new environment footprint and FAIRVIEW operations will continue to task collection for all new and restored circuits.

POC: [REDACTED] S35333, [REDACTED] (FAIRVIEW Collection Manager)

(TS//SI//NF) Mobility Business Records Flow Significantly Increases
Volume of Records Delivered Under BR FISA
By [REDACTED] on 2011-08-30 1440

(TS//SI//NF) On 29 August, FAIRVIEW started delivering Mobility Business Records traffic into MAINWAY under the existing Business Record (BR) FISA authorization. The intent of the Business Records FISA program is to detect previously unknown terrorist threats in the United States through the cell chaining of metadata. This new metadata flow is associated with a cell phone provider and will generate an estimated 1.1 billion cellular records a day in addition to the 700M records delivered currently under the BR FISA. After extensive dialogue with the consumers of the BR data, repeated testing, a push to get this flow operational prior to the tenth anniversary of 9/11, and extensive coordination with external entities via our OGC (to include: FBI, DOJ, ODNI, and FISC) NSA received approval to initiate this dataflow on August 29, 2011. Analysts have already reported seeing BR Cellular records in the Counter Terrorism call-chaining database queries.

POCs: [REDACTED] S3531, [REDACTED] &
[REDACTED] S35324, [REDACTED]

(TS//SI//REL FVEY) FAIRVIEW Tour for Director, Research Directorate
By [REDACTED] on 2012-01-13 0814

(TS//SI//REL FVEY) On 6 January 2012, [REDACTED], Director of NSA's Research Directorate, was provided a tour of FAIRVIEW's East Coast cable station (FRIAR) and FAIRVIEW's centralized processing SCIF (PINECONE). In addition to the site tours, [REDACTED] also received a high level program overview, to include discussion of the various authorities the program operates under, current and future program Cyber plans and some discussion regarding FAIRVIEW's Business Record FISA (BR-FISA) collection. The discussion also included mention of the program's FY12 Strategic Initiatives, a snapshot of the FAIRVIEW's access & collection footprint, clearly depicting the breadth of the access. The day was extremely successful and broadened his understanding of this unique Government/Partner relationship, highlighted the Partner's extreme willingness to help with NSA's SIGINT and Cyber missions and the breadth and depth of not only the program's access, but also the amazing knowledge of the FAIRVIEW partner's workforce.

POC: [REDACTED] FAIRVIEW Tech Director, S3531

(TS//SI//REL FVEY) FAIRVIEW Tour
By [REDACTED] on 2012-03-28 1333

(TS//SI//REL FVEY) On 23 March, S3 and GAO Technical Directors: S3 - [REDACTED], [REDACTED], [REDACTED] GAO - [REDACTED] and [REDACTED], and SV SIGINT Compliance and Architecture Lead [REDACTED], attended the FAIRVIEW partner provided tour of one of the program's east coast cable stations (NASSAU SHORE) and the program's centralized processing SCIF (PINECONE). A short FAIRVIEW overview was provided which led into an in-depth technical discussion regarding the program's vast access & collection infrastructure, the varying data flows (i.e., DNI, DNR, CDRs, etc.) to include program authorities, budget constraints, sensor deployments (ETML, VANGUARD and NETFLOW), and endpoint-midpoint shaping activities and future opportunities in partnership with organizations such as TAO, NCSC and other IC elements such as the FBI, DEA and the CIA. The partner also provided a briefing on company/USG activities outside of FAIRVIEW (i.e., NEST, DIB Pilot) and expounded on current and future program Cyber plans. The day was extremely successful and broadened their understanding of this unique Government/Partner relationship, highlighted the Partner's ability and willingness to help with NSA's SIGINT and Cyber missions, provided insight into the breadth and depth of the program's access and showcased the highly collaborative nature of the FAIRVIEW partner and the value of their intellectual capital.

POC: [REDACTED] FAIRVIEW Program Director, [REDACTED]

(TS//SI//NF) United Nations DNI Collection Enabled
By [REDACTED] on 2012-04-18 0853

(TS//SI//NF) FAIRVIEW and BLARNEY engineers collaborated to enable the delivery of 700Mbps of paired packet switched traffic (DNI) traffic from access to an OC192 ring serving the United Nations mission in New York. The traffic in these links had been encoded using a specific multiplexing technique (GFP). FAIRVIEW engineers and the partner worked to provide the correct mapping, and BLARNEY worked with the partner to correct data quality issues so the data could be handed off to BLARNEY engineers to enable processing of the DNI traffic.

(TS//SI//NF) As of 4 April, BLARNEY began intermittent enablement of DNI traffic for TOPI assessment and feedback. This feedback is being used by the BLARNEY target development team to support an ongoing filtering and throttling of data volumes. While BLARNEY is authorized full-take access under the NSA FISA, collected data volumes would flood PINWALE allocations within hours without a robust filtering mechanism. The initial TOPI feedback has been positive, indicating unique collection to include collection against the email address of the UN General leading the monitoring mission in [REDACTED]. BLARNEY engineers and analysts assessment indicate high quality in both VoIP and VTC collection.

(U//FOUO) POCs: [REDACTED] FAIRVIEW Engineer, [REDACTED], BLARNEY Engineer, [REDACTED], BLARNEY Target Developer, [REDACTED]