PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Reporting* Overview

[redacted] PRISM Collection Manager, S35333

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

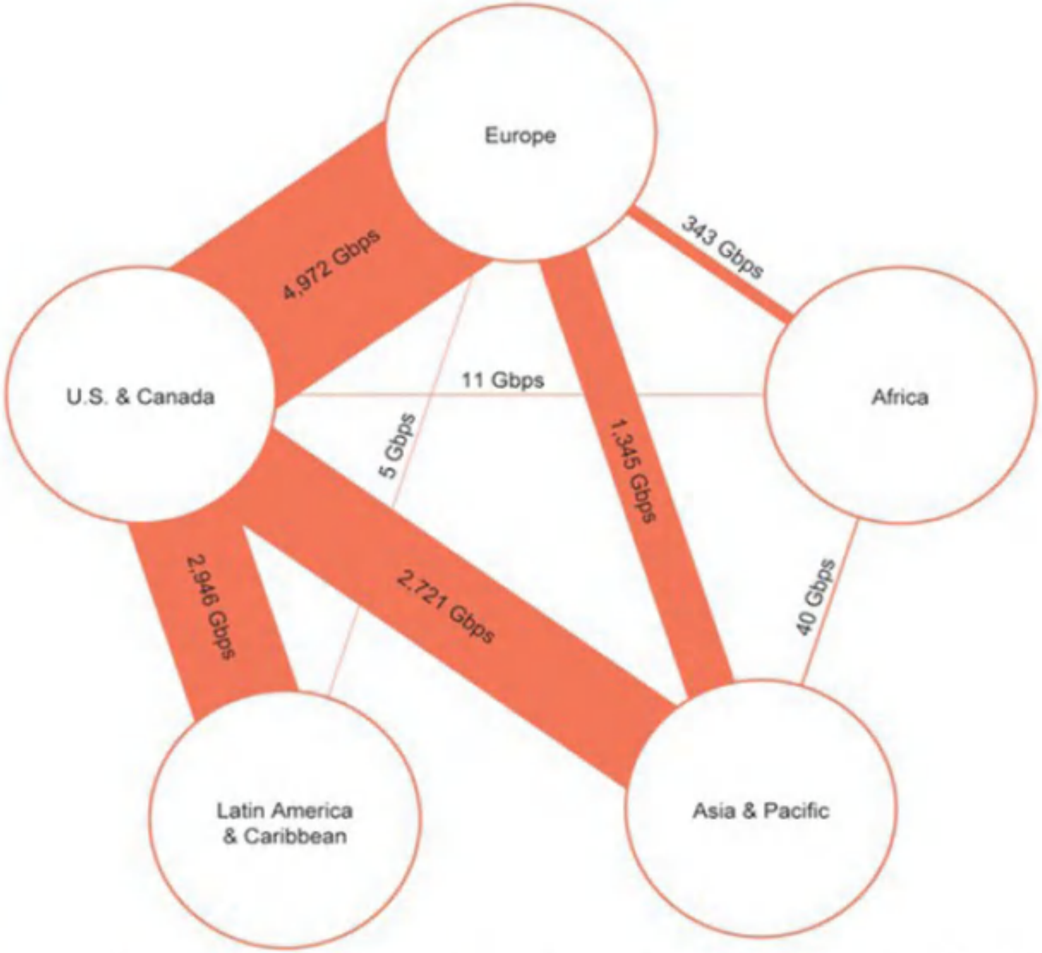
GMail by Google facebook msn Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **__cheapest__** path, **__not the physically most direct__** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

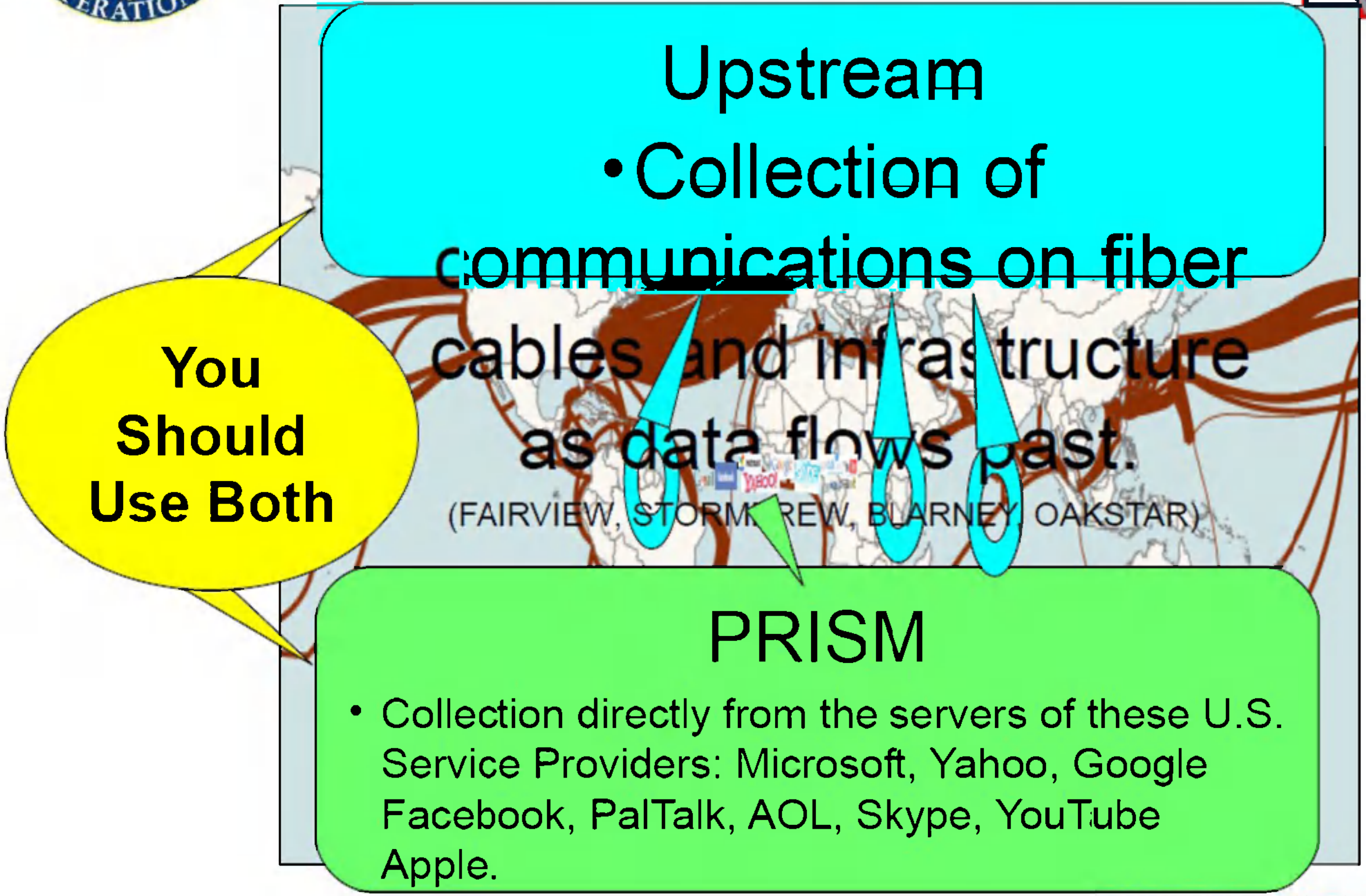


International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

(TS//SI//NF) FAA702 Operations

Two Types of Collection



Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

(TS//SI//NF) FAA702 Operations

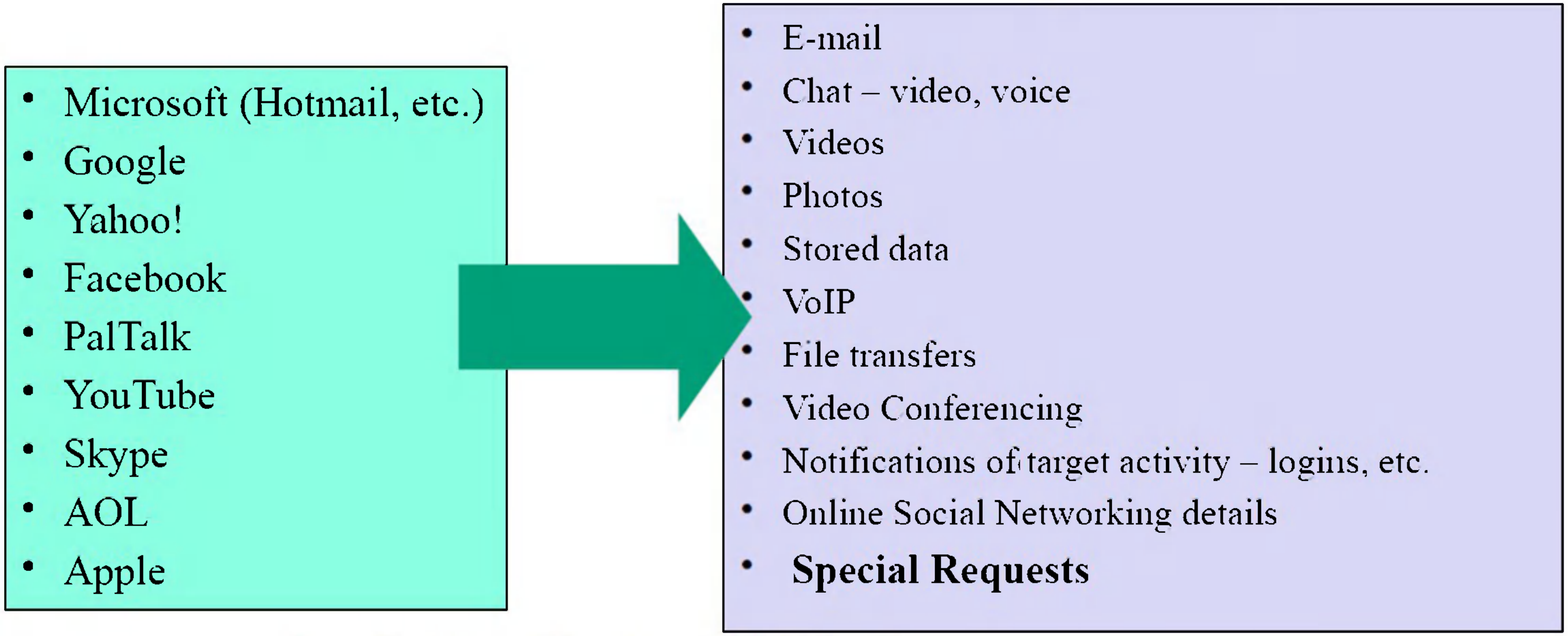
Why Use Both: PRISM vs. Upstream

	PRISM	Upstream
DNI Selectors	✓ 9 U.S. based service providers	✓ Worldwide sources
DNR Selectors	🚫 Coming soon	✓ Worldwide sources
Access to Stored Communications (Search)	✓	🚫
Real-Time Collection (Surveillance)	✓	✓
"Abouts" Collection	🚫	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	🚫 Only through FBI	✓

(TS//SI//NF) PRISM Collection Details

Current Providers

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

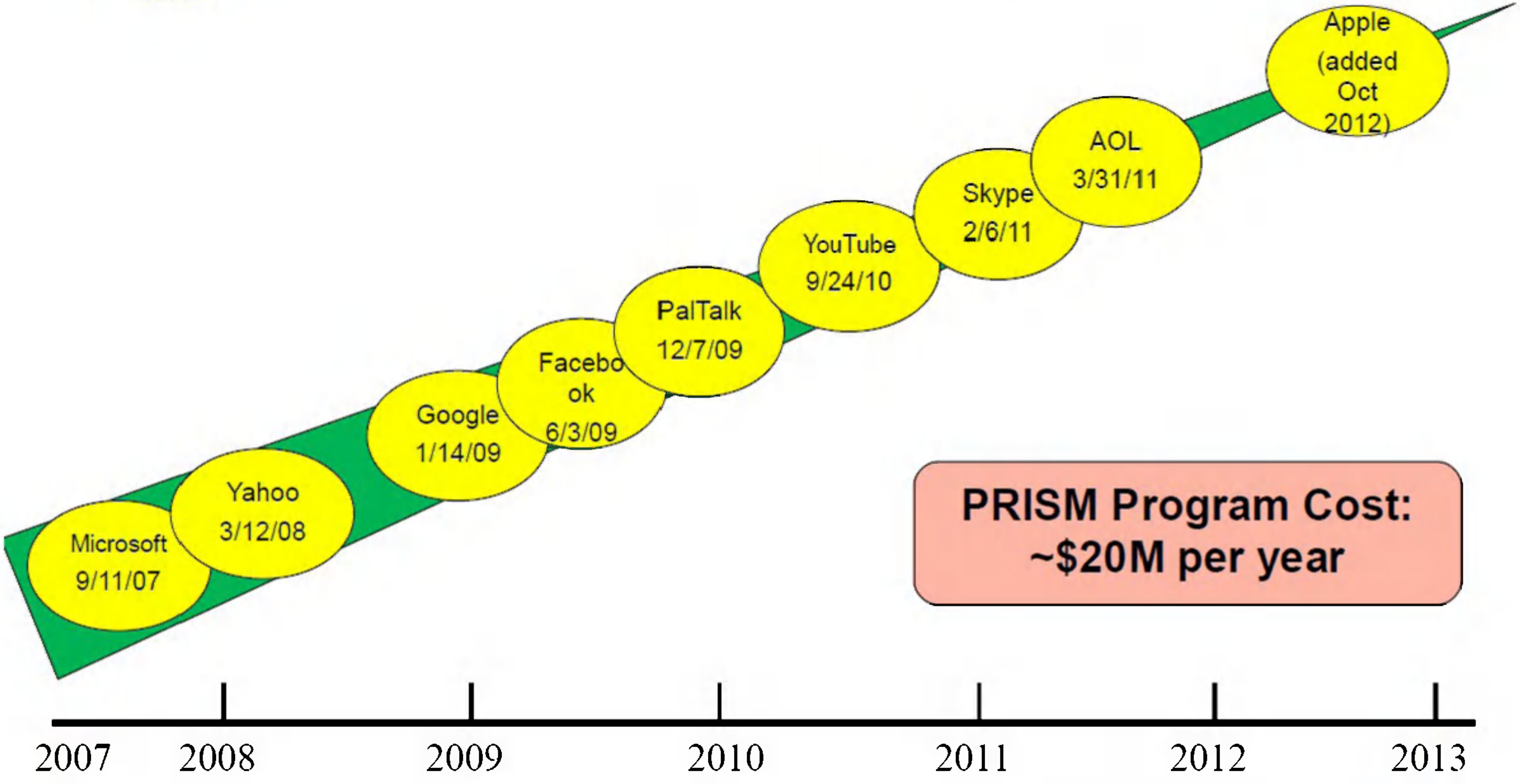


- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



Microsoft
9/11/07

Yahoo
3/12/08

Google
1/14/09

Facebo
ok
6/3/09

PalTalk
12/7/09

YouTube
9/24/10

Skype
2/6/11

AOL
3/31/11

Apple
(added
Oct
2012)

2007 2008 2009 2010 2011 2012 2013

PRISM Program Cost:
~$20M per year

(TS//SI//NF) FAA702 Reporting Highlight

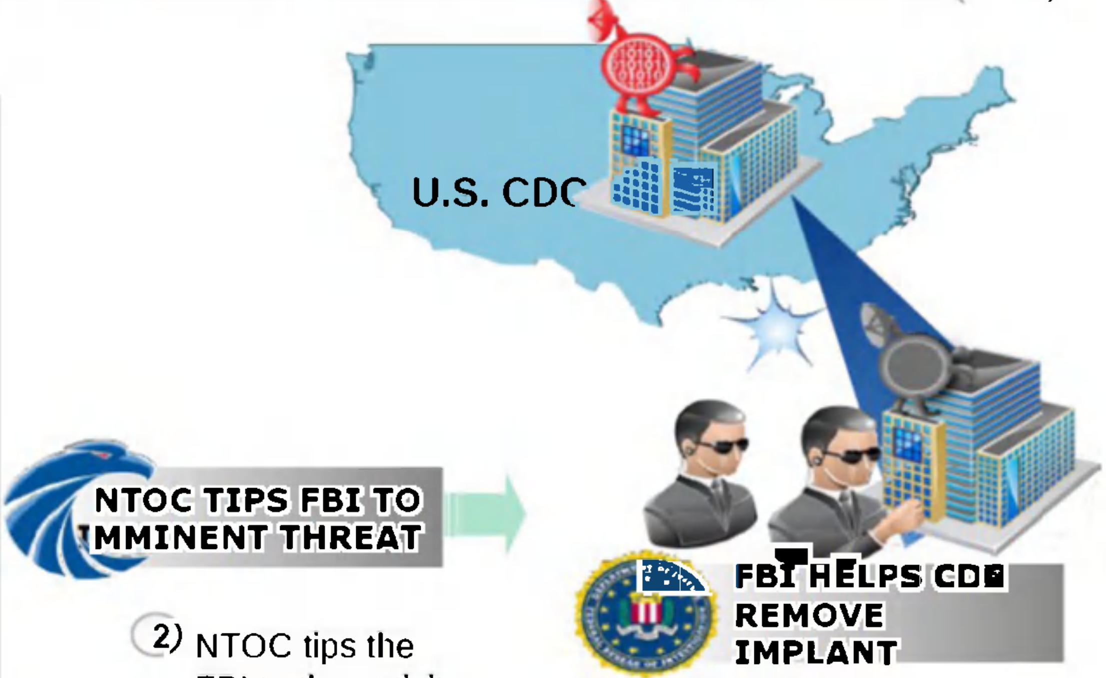
PRISM and STORMBREW Combine To Thwart [redacted]

SAME-DAY NTOC/FBI COLLABORATION

PREVENTS 150GB EXFIL EVENT FROM CLEARED DEFENSE CONTRACTOR (CDC)

2012 14 DEC

[redacted]


U.S. CDC
NTOC TIPS FBI TO IMMINENT THREAT
FBI HELPS CDC REMOVE IMPLANT

2) NTOC tips the FBI to the activity

3) The FBI contacts the CDC and works with them to clean the network.

The victim performed comprehensive actions on the infected network, thus PREVENTING EXFILTRATION on the SAME DAY NTOC DISCOVERED ADVERSARY INTENT

(TS//SI//NF) Some Higher Volume Domains Collected from FAA Passive

In addition to Hotmail, Yahoo, Google, Paltalk, Facebook, Skype, AOL:

Select IP Addresses

[redacted]

[redacted]

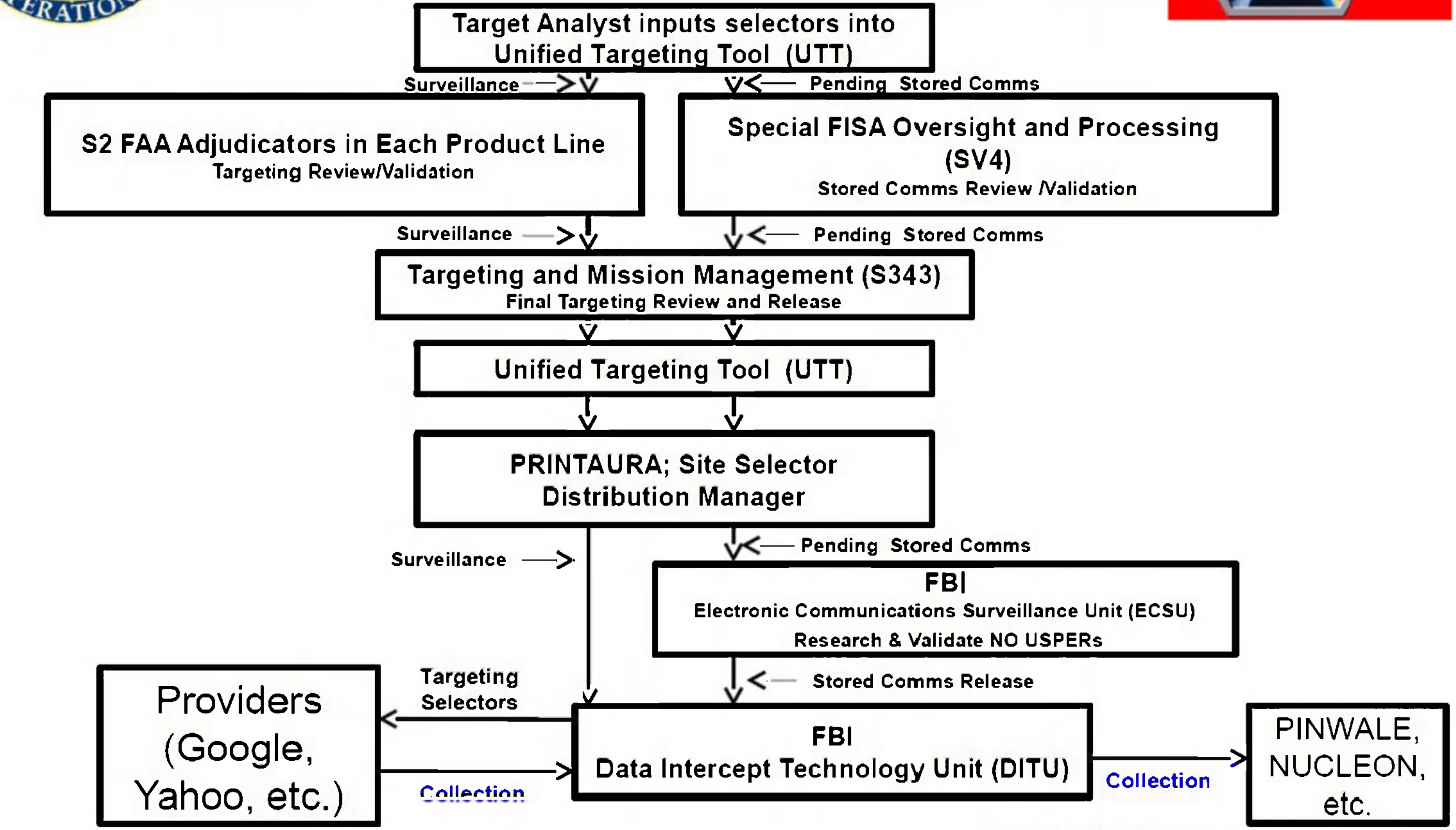
wanadoo.fr

[redacted]

alcatel-lucent.com

[redacted]

(TS//SI//NF) PRISM Tasking Process



Target Analyst inputs selectors into Unified Targeting Tool (UTT)

S2 FAA Adjudicators in Each Product Line
Targeting Review/Validation

Special FISA Oversight and Processing (SV4)
Stored Comms Review /Validation

Targeting and Mission Management (S343)
Final Targeting Review and Release

Unified Targeting Tool (UTT)

PRINTAURA; Site Selector Distribution Manager

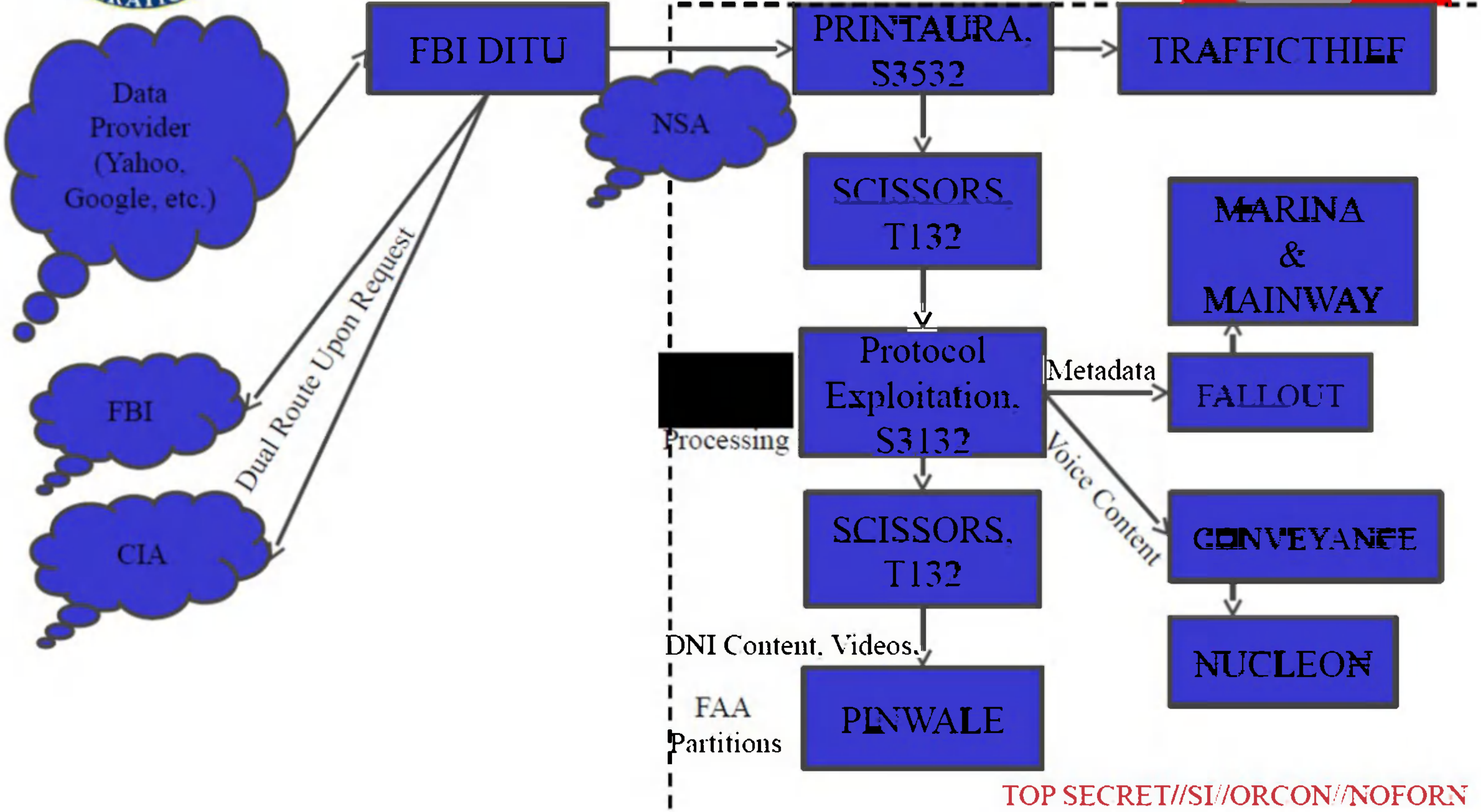
FBI
Electronic Communications Surveillance Unit (ECSU)
Research & Validate NO USPERs

Providers (Google, Yahoo, etc.)

FBI
Data Intercept Technology Unit (DITU)

PINWALE, NUCLEON, etc.

(TS//SI//NF) PRISM Collection Dataflow



Data Provider (Yahoo, Google, etc.)

FBI DITU

NSA

FBI

CIA

Dual Route Upon Request

PRINTAURA, S3532

TRAFFICTHIEF

SCISSORS, T132

MARINA & MAINWAY

[redacted] Processing

Protocol Exploitation, S3132

Metadata

FALLOUT

Voice Content

CONVEYANCE

SCISSORS, T132

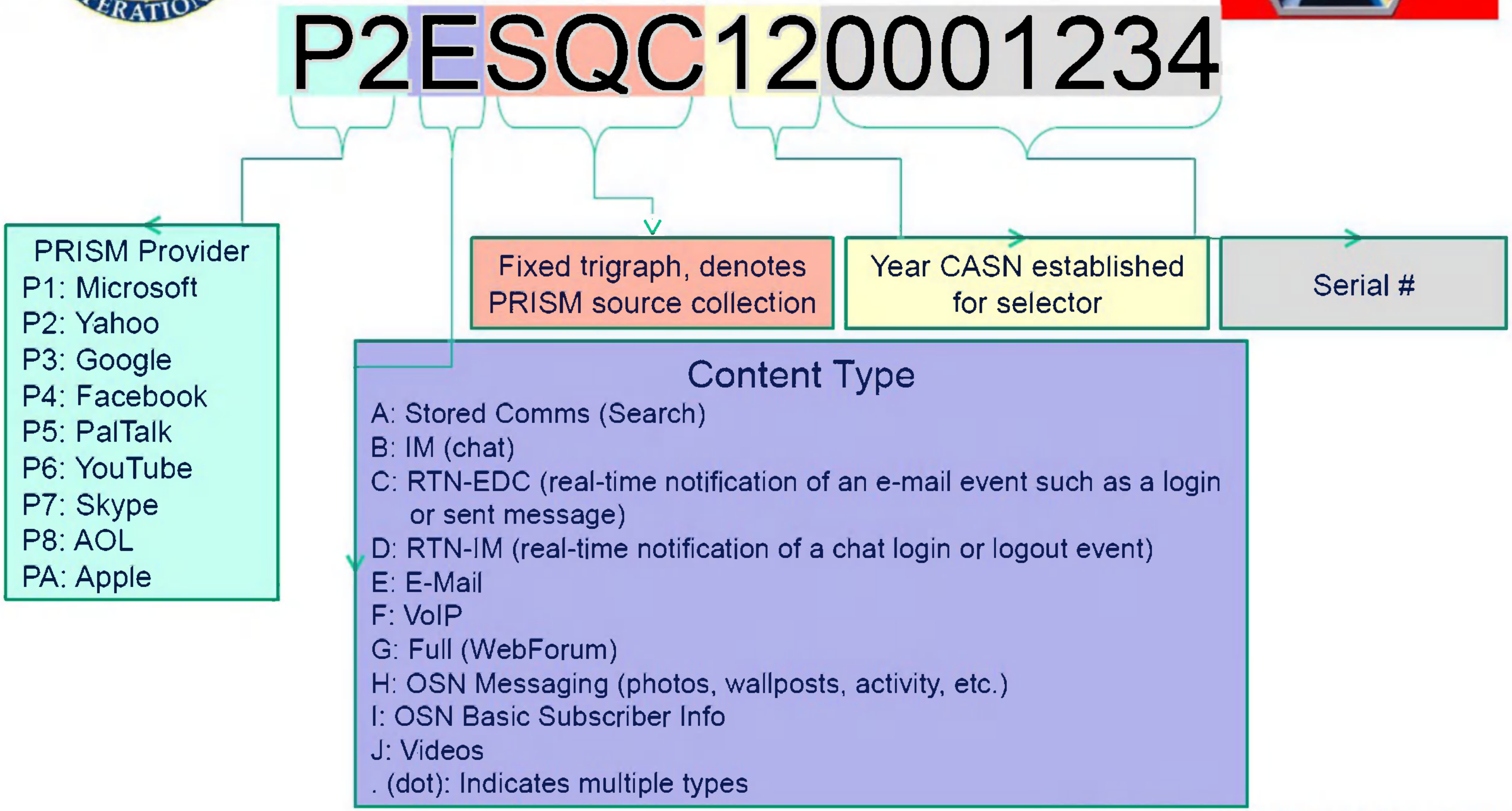
NUCLEON

DNI Content, Videos,

FAA Partitions

PINWALE

(TS//SI//NF) PRISM Case Notations



P2ESQC120001234

PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type

A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types