



# (U//FOUO) AURORAGOLD



(S//SI//REL) **Project Overview:** The mission of the AURORAGOLD (AG) project is to maintain data about international GSM/UMTS networks for the Wireless Portfolio Program Office (WPMO), the Target Technology Trends Center (T3C/SSG4), and their customers. Analysis of this data supports:

- a) An understanding of the current state,
- b) Trending, or time-series analysis, from the past through to the future, and
- c) Forecasting of the evolution of global GSM/UMTS-based networks.

This analysis and developmental activity is currently focusing only on GSM/UMTS infrastructure, voice-data convergence, UMTS technology migration, and UMTS technology deployments. Coincident beneficiaries of this mission are, among others, other NSA SIGDEV elements, protocol exploitation elements, and Five-Eyes Partner SIGDEV organizations.

(C//REL) **Alignment:** Supports NSA's and SID's imperative to "Know the Future."

(C//REL) **Sponsors:** WPMO/S3W

(C//REL) **Customers:** WPMO/S3W; T3C/SSG4; Various S3 collections organizations; numerous IC organizations

(C//REL) **Architecture and Infrastructure:** Custom-built application based on OZONE framework, using GOLDENCARRIAGE corporate servers for all application and data storage



# (U//FOUO) AURORAGOLD



## (S//SI//REL) **Corpus:**

Will contain:

- Unclassified: Complete replica of Informa Telecoms and Media's World Cellular Information Service (WCIS) queryable database to eventually compare data against that collected from SIGINT
- Classified: SIGINT-collected IR.21 (International Roaming agreements) documents from around the world, parsed of their information, analyzed, and giving users the ability to trend this information over time (time-series analysis). In addition, e-mail selectors from within IR.21s and from SIGINT metadata captured, analyzed and managed back into the SIGINT system for enhanced collection

## (C//REL) **Content:**

- Portion of the WCIS data available via NSANet GUI; remainder to be completed within 2-3 months
- Currently, Phase 1 contains a small database of worldwide wireless networks being compared against IR.21s from SIGINT to establish our "baseline"

## (C//REL) **Capabilities:**

- Soon, complete WCIS repository to be copied to NSANet for querying by all NSA and 2P Partners
- Later, agile querying through entire IR.21 and WCIS databases, with capability to perform time-series analysis via visualization application



# (U//FOUO) AURORAGOLD Repository



TOP SECRET//SI//REL TO USA, FVEY

**AURORAGOLD**

This product may contain copyrighted material; authorized use is for national security purposes of the United States Government only. Any reproduction, dissemination, or use is subject to the NSA usage policy and the original copyright.

(S//RF1) The mission of the AURORAGOLD (AG) project is to maintain data about international UMTS networks for the Wireless Portfolio Program Office (WPPO), the Target Technology Trends Center (T3C), and their customers. Analysis of this data supports:

- a) An understanding of the current state,
- b) Trending, or time series analysis, and
- c) Forecasting of the evolution of global UMTS-based networks.

This analysis and developmental activity will focus on UMTS infrastructure, voice-data convergence, UMTS technology migration, and UMTS technology deployments. Coincident beneficiaries of this mission are, among others, other NSA SIGDEV elements, protocol exploitation elements, and Five-Eyes Partner SIGDEV organizations.

Networks & Suppliers 7/2010	Handsets & Devices 6/2010	Network Features 1/2011	Network Coverage 1/2011	Licenses 1/2011	Licensed Spectrum 1/2011
-----------------------------	---------------------------	-------------------------	-------------------------	-----------------	--------------------------

Networks & Suppliers

↑

Handsets & Devices

↑

Network Features

↑

Network Coverage

License

↑

Licensed Spectrum

TOP SECRET//SI//REL TO USA, FVEY

Done

Start | Inboxes - Microsoft Outlook | SSG4 Projects Overview | Aurora Gold - Window... | Z:\Wiki\_Development\Lo...

Internet | 100% | 3:22 PM Monday



# (U//FOUO) AURORAGOLD



## (C//REL) Demonstration Script

- (Only capability currently available is basic querying against small portion of WCIS database)
- Go to [REDACTED]
- Click on any of the brown boxes
- Select your search criteria
- Select your query result criteria
- Click "Submit"
- View the results





(U//FOUO)

# ***AURORAGOLD***

**Target Technology Trends Center/T3C  
support to WPMO**

---

**Overall briefing classification: S//SI//REL TO USA, FVEY**



(C//REL TO USA, FVEY)

## **Two synergistic efforts:**

Trending and forecasting of global wireless and cellular networks

### ***AURORAGOLD***

- Data gathering and analytics on GSM/UMTS networks

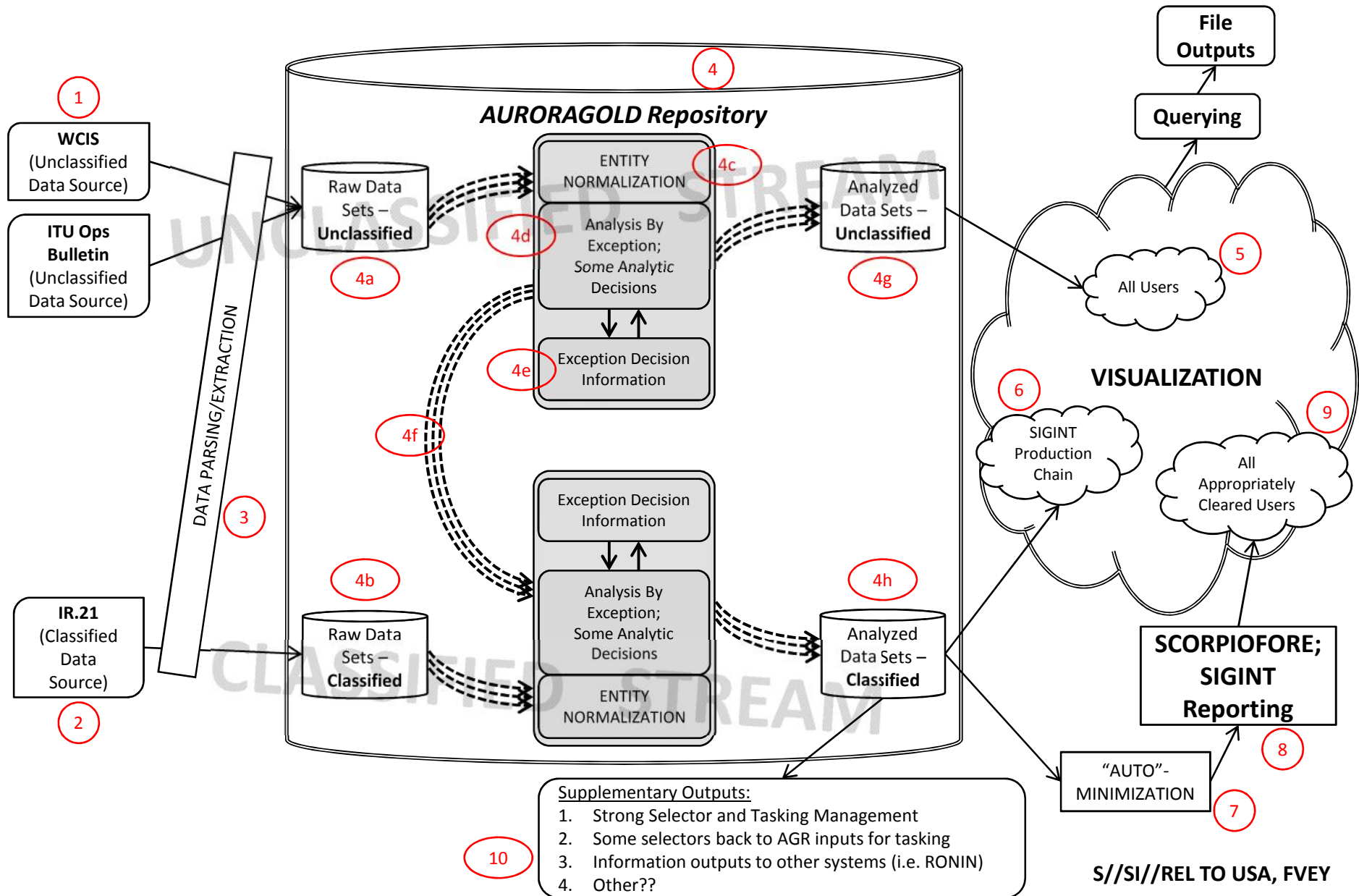
### ***“Auto”-Minimization***

- Automated minimization capability to ensure compliance with NSA reporting policy

# AURORAGOLD DATA FLOW & PROCESS OVERVIEW



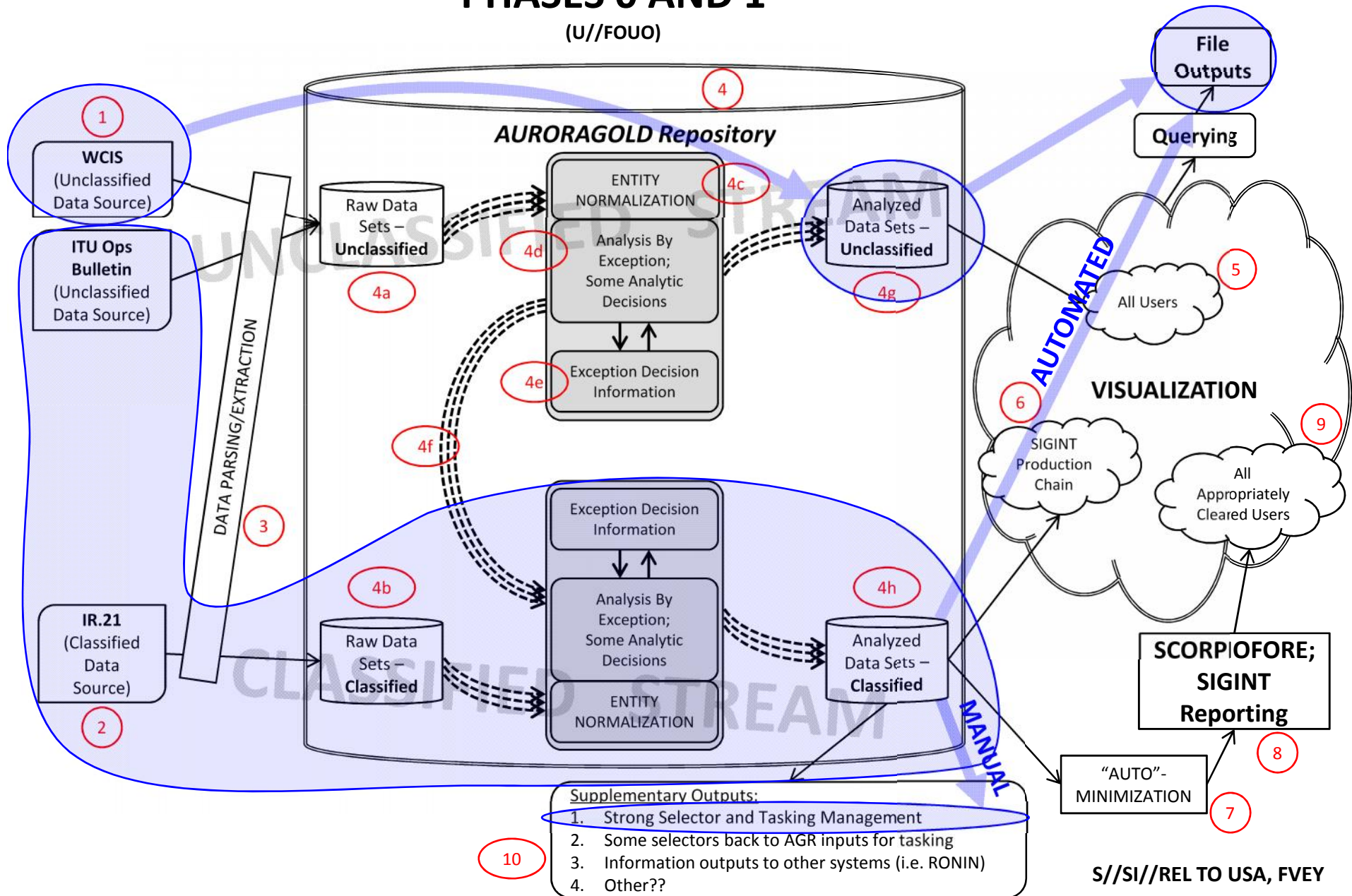
(U//FOUO)



S//SI//REL TO USA, FVEY

# AURORAGOLD DATA FLOW & PROCESS OVERVIEW: PHASES 0 AND 1

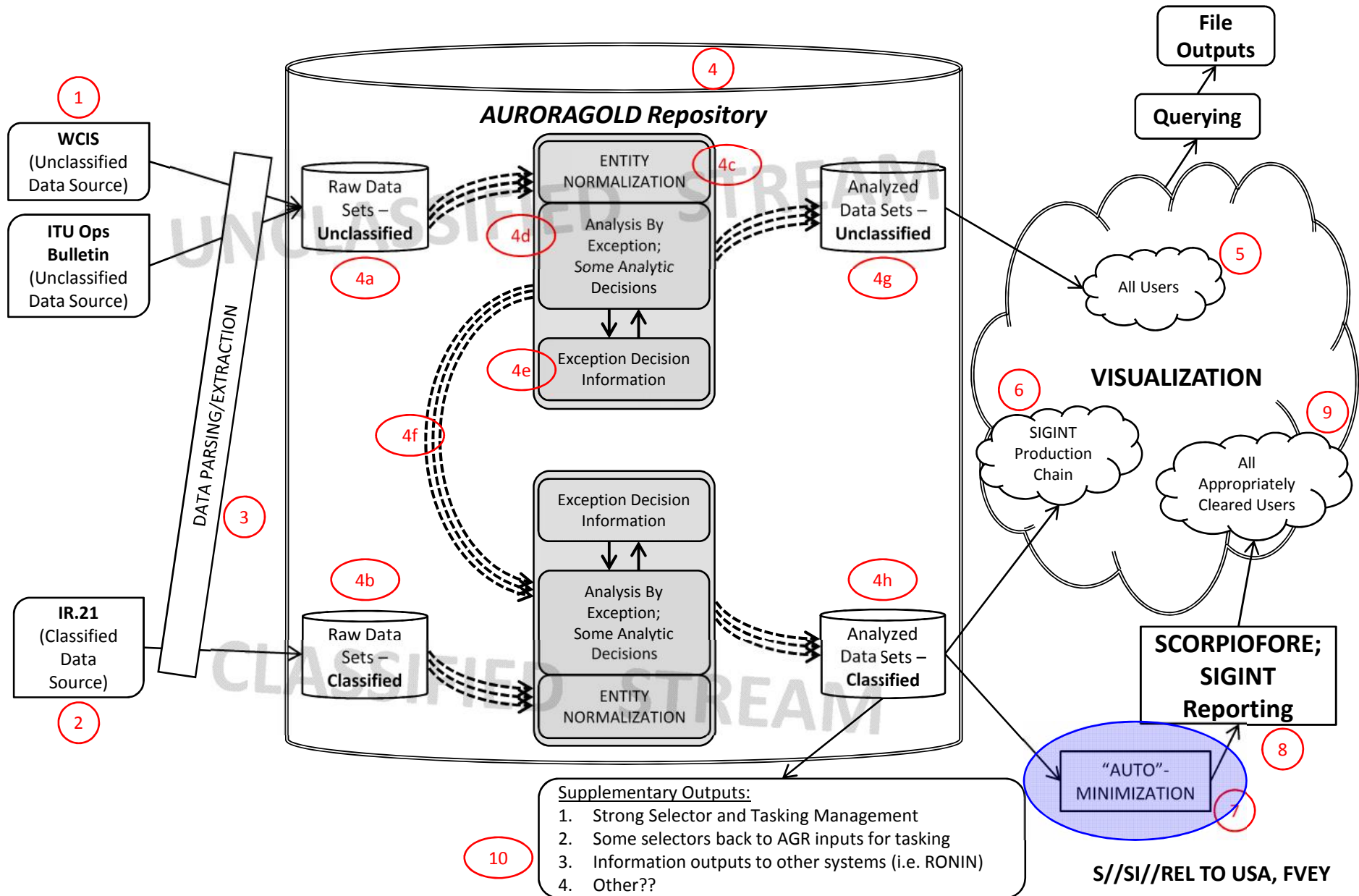
(U//FOUO)



# AURORAGOLD DATA FLOW & PROCESS OVERVIEW



(U//FOUO)



S//SI//REL TO USA, FVEY





# AURORAGOLD

## NOW:

- GSM technology family from unclassified data
- Parsing IR.21 documents from SIGINT
- Basic analytics
- Basic auto-sourcing

## FUTURE:

- Additional fields
- Additional sources
- Entity normalization
- Complex analytics
- Advanced auto-sourcing
- **“Auto”-Minimization**
- SCORPIOFORE reporting
- Visualizations enabling time-series analyses

(C//SI//REL TO USA, FVEY)

## RISKS:

- Data sources and ingest
- Expanding capability to other wireless technologies





## WORKING AID (UPDATED 17 MAY 2012)

(U//FOUO) AURORAGOLD is a team of SSG4 analysts, developers and wireless SMEs working on:

- (S//SI//REL) Database of Mobile Network Operators (MNOs), networks, and PWIDs collected from GSM/UMTS/LTE roaming documents (IR.21s),
- (S//SI//REL) Target development effort against MNOs, roaming hubs, and GSM Association (GSMA) working groups, and
- (U) Fusion of open source, licensed, commercial data with SIGINT to answer wireless needs.

### **(S//SI//REL) Sample SIGINT (IR.21) Queries**

- (S//SI//REL) What IR.21s have we seen for networks within a country or set of countries?
- (S//SI//REL) What IR.21s have we seen for networks managed by a mobile network operator?
- (S//SI//REL) What IR.21s have we seen for a particular network or set of networks?

### **(U) Sample Open Source (Licensed Commercial Data) Queries**

- (S//SI//REL) What are all of the cellular network operators within a country currently in service?
- (S//SI//REL) What suppliers have sold equipment to which operators within a country?
- (S//SI//REL) What networks are currently in service/planned within a country for each operator?
- (S//SI//REL) Which network technology equipment exists within a country for each operator?

- (S//SI//REL) What is the network name for each network within a country for each operator?
- (S//SI//REL) When was each network placed into service for each operator within a country?
- (S//SI//REL) What cellular network technology (e.g., GSM, W-CDMA, HSPA, etc.,) is in service for each operator in a country?
- (S//SI//REL) Which frequency spectrum bands are being used by which operators in a country?
- (S//SI//REL) What 4G/LTE networks are currently in service/planned for each operator within a country?
- (S//SI//REL) What CDMA or CDMA Wireless Local Loop networks are currently in service/planned for each operator within a country?
- (S//SI//REL) What network license auctions are planned within a country?

Derived From: NSA/CSSM 1-52 Dated: 20070108
---

**(S//SI//REL) Some IR.21 Fields Useful to SIGINT**

<b>(U) IR.21 Field</b>	<b>(U) What is it?</b>	<b>(U) How is it used?</b>
<b>Mobile Country Code (MCC)/ Mobile Network Code (MNC)</b>	(U) A decimal digit code which uniquely identifies a mobile network. The MCC which identifies the country is used as the first three digits of any user's IMSI, followed by the two digit MNC which identifies the network within that country.	(U) Provide unique identification of networks to identify network boundaries, interfaces, protocols, software, hardware, etc.
<b>Mobile Subscriber Integrated Services Digital Network Number (MSISDN)</b>	(U) A number uniquely identifying a subscription in a GSM or a UMTS mobile network (the telephone number to the SIM card in a mobile/cellular phone).	(U) Allow identification of real phone number dialed
<b>TADIG codes</b>	(U) A number allocated by the GSMA for use as primary identifiers, both within file contents and file names. Also used as a more generic entity identifier in the mobile industry	(U) Identify the network for billing purposes and help identify targets
<b>Signaling Connection Control Part (SCCP)</b>	(U) A network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities in Signaling System 7 telecommunications networks	(U) Provides routing information within the Public Land Mobile Network and provides access to applications such as 800-call processing and calling card processing to identify targets and other information
<b>Subscriber Identity Authentication</b>	(U) This field indicates whether or not authentication is performed for roaming subscribers at the start of GSM service and the type of A5 cipher algorithm version in use.	(S//SI//REL) It would also show the emergence of new cipher algorithms and support target analysis, trending and the development of exploits.
<b>Mobile Application Part (MAP)</b>	(U) A SS7 protocol which provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. The Mobile Application Part is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Centre, Short message service center and Serving GPRS Support Node (SGSN).	(S//SI//REL) Provides a clearer understanding of network features when roaming agreement information is published. Current information about subscribers, mobility management and applications can be used for targeting and target development.
<b>Network Element</b>	(U) Specific network components, their manufacturer, software & hardware versions, etc.	(S//SI//REL) This specific information is necessary for targeting and exploitation. Includes core and

<b>Information</b>		radio interface information.
<b>Packet Data Services Information</b>	(U) Packet Data Services identifies the affected GPRS networks. An Access Point Name is also included in this information. APNs can identify the type of service provided by GPRS networks provided to mobile users. APNs also help identify the network and operator's packet network involved in the IR.21 and could be used for targeting.	(S//SI//REL) This data element also provides information on the WAP gateway being access and multimedia messaging services gateway IP addresses which is useful for target development. Insight into the GPRS Tunneling Protocol versions being used within the networks is provided as well. GPRS, EDGE and HSPA technologies are covered.



# (U//FOUO) AURORAGOLD Working Group

(S//SI//REL) Shaping understanding of  
the global GSM/UMTS/LTE landscape

SIGDEV Conference – 6 June 2012

This briefing is classified:  
TOP SECRET//SI//REL TO FVEY

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20370501



# Agenda



(U)

- (U//FOUO) What is AURORAGOLD?
- (U) Why come to us?
- (U) Our value proposition...
  - (S//SI//REL) Primary source mobile network information
  - (S//SI//REL) First-hand insight into industry changes
- (U//FOUO) Targeting efforts
- (U) Notable successes
- (U) Future plans
- (U) Discussion!





# What is AURORAGOLD?



(U//FOUO)

(U) Team of analysts, developers, and wireless SMEs working on:

- (S//SI//REL) Database of Mobile Network Operators (MNOs), networks, and PWIDs from collected GSM/UMTS/LTE roaming documents (IR.21s)
- (S//SI//REL) Target development effort against MNOs, roaming hubs, and working groups
- (U) Fusion of open source, commercial data with SIGINT to answer wireless needs



# Why come to us?



(U)

- (S//SI//REL) Extensive, global IR.21 data vetted by SSG4 analysts:
  - **701 networks of estimated 985** (as of 15 May 2012)
  - First-hand SIGINT information direct from MNOs
- (S//SI//REL) Most comprehensive set of IR.21-related email selectors and keyword-based tasking:
  - **1201 actively managed email selectors** (as of 15 May 2012)
- (U//FOUO) Foundation for worldwide mobile wireless network trending and forecasting
  - Includes visibility into changing industry standards and practices



# How can we help you?



(U)

(S//SI//REL) Example: "AFRICOM IKD-OPS requires information concerning the SMS Gateway domains for: Libyana mobile (libyana.ly) and Al Madar Al Jadid (almdar.ly). We believe these are the only two mobile providers in Libya but if you have information to the contrary please let us know."

3 March 2011





# We've done the research



(U)

- (S//SI//REL) Quickly identified collected IR.21s
- (U//FOUO) Pushed information out to customer through product reporting

DOCN 000028528  
 ZNY ZNY MMIVX  
 ZKZK ZKZK RR SOL DE  
 PDTG R 162037Z MAR 11  
 FM FM DIRNSA  
 CLAS T O P S E C R E T UMBRA US/UK/CAN/AUS/NZ EYES ONLY QQQQ  
 XXMM XXMMENP01FOO11075

SERI SERIAL: 3/00/506998-11

TAGS TAGS: LIC CCOM CLOG COEF CORG CPER CTEC CTPH LI

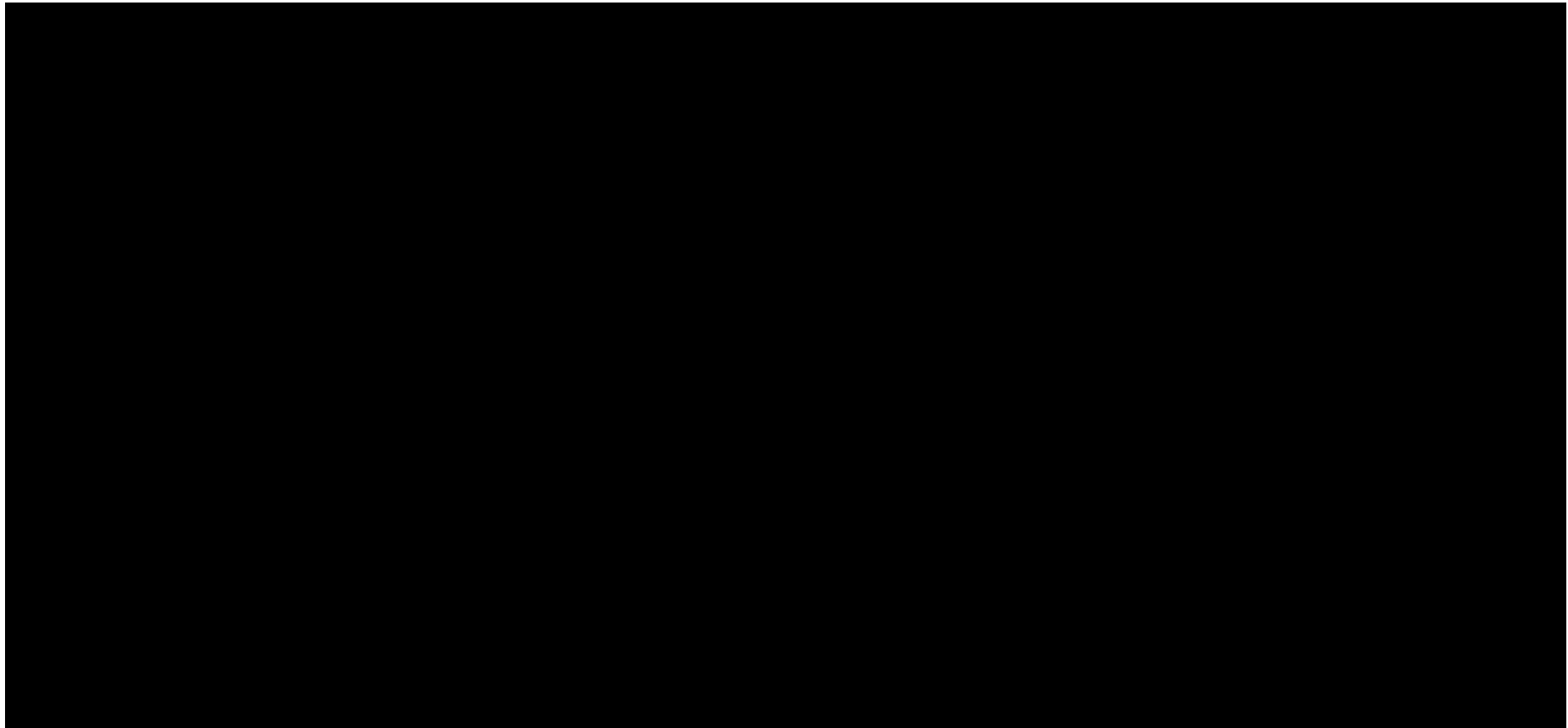
SUBJ SUBJ: Libya/Telecommunications: Two Libyan Mobile Phone Companies  
 Provide Updated Network Information, June and December 2010  
 (S//SI//REL TO USA, FVEY)



# SIGINT Value – Al Madar IR.21



(S//SI//REL)



Extracted from 3/00/506998-11



# SIGINT Value – Al Madar IR.21



(S//SI//REL)

Vendor Information	
BSS vendor(s) and SW/HW version:	Ericsson
HLR vendor(s) and SW/HW version:	Ericsson
MSC/VLR vendor(s) and SW/HW version:	Ericsson
SMSC vendor(s) and SW/HW version:	Alcatel-Lucent V 3.1
SGSN vendor(s) and SW/HW version:	Ericsson R7
GGSN vendor(s) and SW/HW version:	Ericsson R4
MMSC vendor(s) and SW/HW version:	Ericsson MMC 5.0
IN vendor(s) and SW/HW version:	Alcatel-Lucent

SMSC Information	
SMSC GT addresses <sup>9</sup> :	[REDACTED]

GPRS Information	
APN Operator Identifier	
List of APN	
WED	APN
	Username
	Password
	ISP DNS IP address (primary)
WAP	ISP DNS IP address (secondary)
	APN
	Username
	Password
MMS	WAP Gateway IP address
	WAP Server URL
	Port
	APN
GTP version	Username
	Password
	WAP Gateway IP address for MMS
	Messaging Server URL
BSS information (optional field)	Port
	SGSN
	GGSN
Contact person(s) for GPRS (optional field)	

MMS Interworking Information	
Domain name of MMSC	[REDACTED]
IP address range for MMSC	[REDACTED]
IP address(es) of incoming MTA	[REDACTED]
IP address(es) of outgoing MTA	[REDACTED]
Max. size of MMS allowed	[REDACTED]
Delivery Report allowed?	[REDACTED]
Read Report allowed?	[REDACTED]
Contact person(s) for IW MMS: (optional field)	[REDACTED]
MMS IW Hub Provider(s) GT addresses:	[REDACTED]
MMS IW Hub Provider(s) Name(s):	[REDACTED]

Extracted from 3/00/506998-11





# IR.21s in AURORAGOLD



(S//SI//REL)

## 1.8.3 ROAMING DATA BASE

Operator name	AL MADAR AL JADID
Technology	GSM 900/1800
Country (Abbreviated according to ISO 3166)	Libya LBV

ROUTING INFORMATION		
CCITTE.164 Number series:	Country Code (CC)	National Destination Code (NDC)
MSISDN Number range(s):	218	91
Network nodes Global Title number range(s):	218	91
E.212 Number series:	Mobile Country Code (MCC)	Mobile Network Code (MNC)
	606	01
E.214 Mobile Global Title (MGT)	Country Code of MGT (CC)	Network Code of MGT (NC)
	218	91
Does Number Portability apply <sup>1</sup> ?	No	

## International Roaming Coordinator:

Eng. [REDACTED]  
 IR Coordinator  
 T: [REDACTED]  
 Fax: [REDACTED]  
 Email: [REDACTED]@alمدار.ly

Eng. [REDACTED]  
 IR Coordinator  
 T: [REDACTED]  
 Fax: [REDACTED]  
 Email: [REDACTED]@alمدار.ly

Eng. [REDACTED]  
 IR Coordinator  
 T: [REDACTED]  
 Fax: [REDACTED]  
 Email: [REDACTED]@alمدار.ly

Eng. [REDACTED]  
 IR Coordinator  
 T: [REDACTED]  
 Fax: [REDACTED]  
 Email: [REDACTED]@alمدار.ly

Extracted from 3/00/506998-11



# We monitor the industry



(S//SI//REL)

- (S//SI//REL) Visibility into changing standards and practices for:
  - Roaming
  - Signaling
  - Billing
  - Interoperability
- GSM Association (GSMA), a Swiss association that drives the GSM/UMTS/LTE space



# Roaming Agreement EXchange (RAEX)



(S//SI//REL)

- (U) Next-generation roaming exchange process
- (U) Well-defined XML schemas instead of semi-structured data in multiple formats
- (U) Email likely gives way to SSL sessions with central server(s)

(S//SI//REL)	SIGINT Access	SIGINT Value	Automated Analytics
Old IR.21s	Easy	Great	Nearly impossible
RAEX IR.21s	Difficult	Even greater!	Easy!



# Targeting Efforts



(U//FOUO)

- (S//SI//REL) MNO roaming coordinators, hubs, GSMA working groups, ROAMSYS
- (S//SI//REL) ~100% of MNOs in WPMO's Top 20

Category	Contains...
4002	IR21 senders/receivers
3918	GSMA and SIGDEV

Tag	Contains...
AGIR21	IR21 senders/receivers
AG_USER	Individual (usually sender)
AG_ALIAS	Alias (usually receiver)
MCC/MNC [###][###]	IR21 s/r for given network
AGRAEX	RAEX working groups
roaming hub	Roaming hub contacts





# Email Address Selectors



(S//SI//REL)

**Filter Criteria**

Org: [ ] Team: [ ] Batch Taskable: All [v]

Designator: [ ] Zipcode: [ ] Place Name: [ ]

Category: [ ] Tag: MCC/MNC [ ] Realm: All [v] Selector: [ ]

Target Type: All [v] Targeting Nationality: IR [v] Target Name: [ ]

Targeting Location: IR [v] Target Shareable Name: [ ]

Targeting Status: Tasked [v] Create Date >= [ ] Create Date <= [ ]

**Selector Information** Task Create New TR

Display: 25 [v] Page 1 of 1 Total Records: 6

Select All / Clear All	Normalized Selector	Target Shareable Name	Interest	Targeting Interest	Targeting Status	Task
<input type="checkbox"/>	[redacted]:emailAddr>	[redacted]	1		✗	Task
<input type="checkbox"/>	[redacted]:emailAddr>	[redacted]	1		✗	Task
<input type="checkbox"/>	[redacted]:emailAddr>	[redacted]	1	1	✓	Task
<input type="checkbox"/>	[redacted]:emailAddr>	[redacted]	1		✗	Task
<input type="checkbox"/>	[redacted]:emailAddr>	[redacted]	1	1	✓	Task
<input type="checkbox"/>	[redacted]:emailAddr>	[redacted]	1	1	✓	Task

UTT v3.2 SP1 - Task Selector Search

Dynamic Page -- Highest Possible Classification is TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



# Notable Successes



(U)

- (TS//SI//REL) Characterization of IR.21 collection from 67 high-priority networks (DSD)
- (TS//SI//REL) Most recent IR.21s from Egypt (S2E)
- (S//SI//REL) Assessment of IR.21 collection related to a possible new Chinese network (S2B)
- (S//REL) Sole source of IR.21 collection, ingest, and processing for RONIN; >200% improvement (NAC)
- (S//SI//REL) Working toward enterprise sharing of licensed, commercial data
  - Today: WiMAX data with JUBILEECORONA (S3516)
- (TS//SI//REL) Reporting on GSMA standards and practices





# Future Plans



(U)

- (S//SI//REL) RAEX IR.21 collection and ingest providing more query possibilities including:
  - LTE information
  - Technologies/Equipment
  - Frequencies
- (S//SI//REL) AURORAGOLD user interface enabling SIGINT production chain access for querying and trending
- (S//SI//REL) NKB partnership



# Discussion



(U)

- (S//SI//REL) What are your ideas, suggestions, and analytic needs with respect to:
  - roaming and network information discovery and development?
  - GSMA's standards setting activities?
- (S//SI//REL) What are we missing? Are there data elements we should seek out to help meet your needs?



# Work with us!

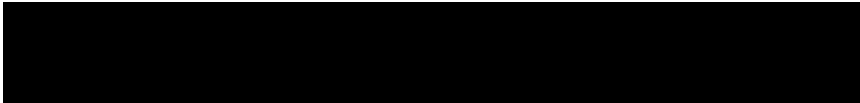


(U)

- (U//FOUO) To contact the AURORAGOLD team with an RFI, please use GLOBAL TIPPER

“go GT”



- (U//FOUO) WikiInfo: “wi AURORAGOLD”
- (U//FOUO) Email: 

(U//FOUO) AURORAGOLD

# **(U) BACKUP SLIDES**



# AG/GSMA Reporting



(S//SI//REL)

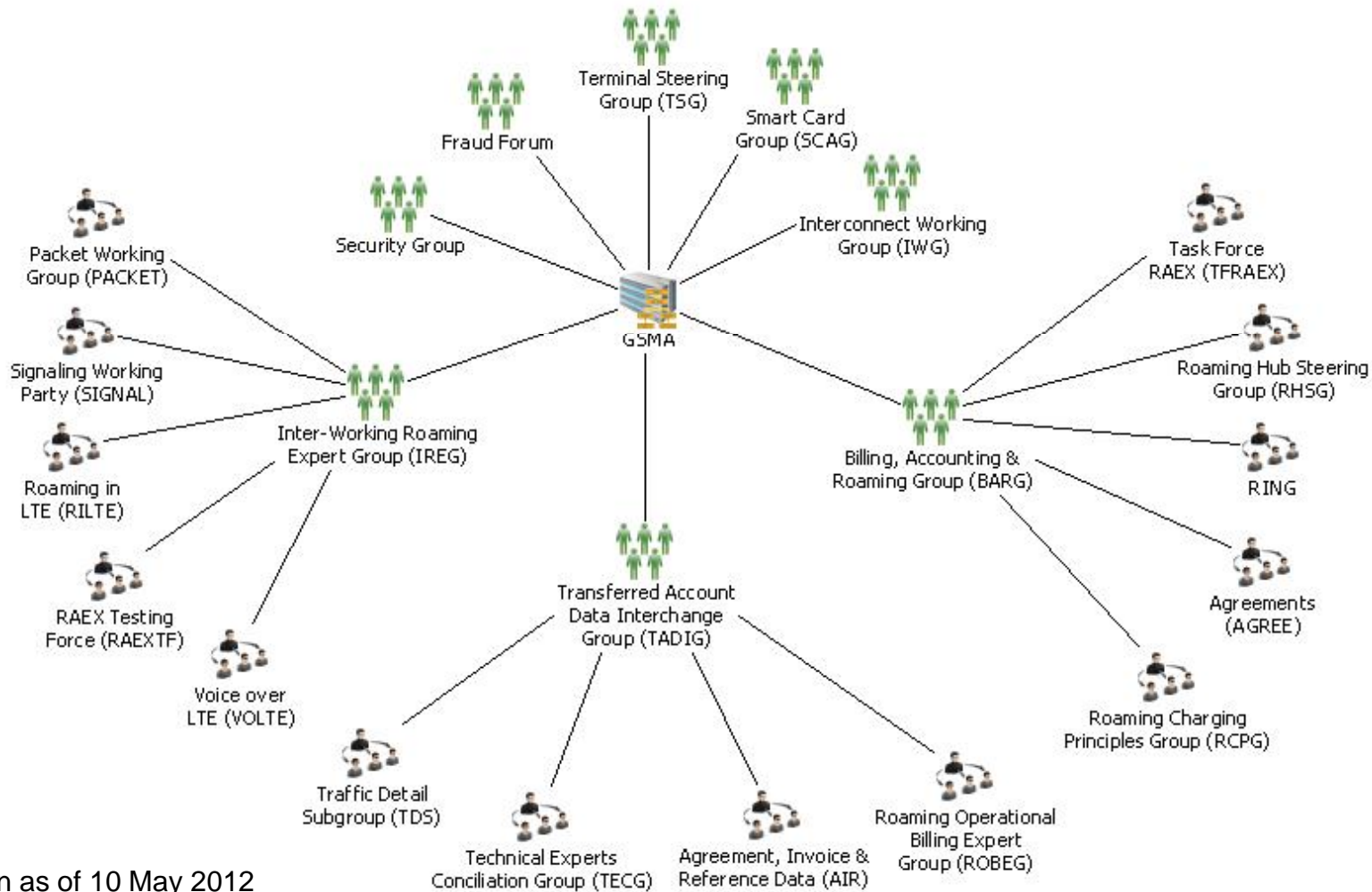
Serial	Topic
3/00/506998-11	(S//SI//REL) Libyan MNO information
3/00/556211-11	(S//SI//REL) Launch of RAEX; ROAMSYS and GSMA
3/00/515656-12	(S//SI//REL) GSMA standards releases/changes for 2012 (RAEX IR.21 and others)
2/00/502330-12	(S//SI//REL) GSMA database of Type Allocation Codes (TACs)



# GSMA Working Groups



(S//SI//REL)



(U) Known as of 10 May 2012



# IR.21 Data Extraction



(S//SI//REL)

## (U) Content

Field	AG	R
MCC/MNC	x	x
Operator name	x	x
Operator country	x	x
Email addresses	x	
Access point information		x
Autonomous system number		x
DNS names & IPs		x
Inter PLMN backbone IPs		x
GPRS Roaming Exchange (GRX)		x

## (U) Metadata/SRI

Field	AG	R
SIGAD	x	x
Case notation	x	x
PWID	x	x
PINWALE Date Time Group	x	x
PINWALE category & keywords	x	
Email "From" & date	x	
Source & destination IP	x	
Filename	x	
PDDG		x



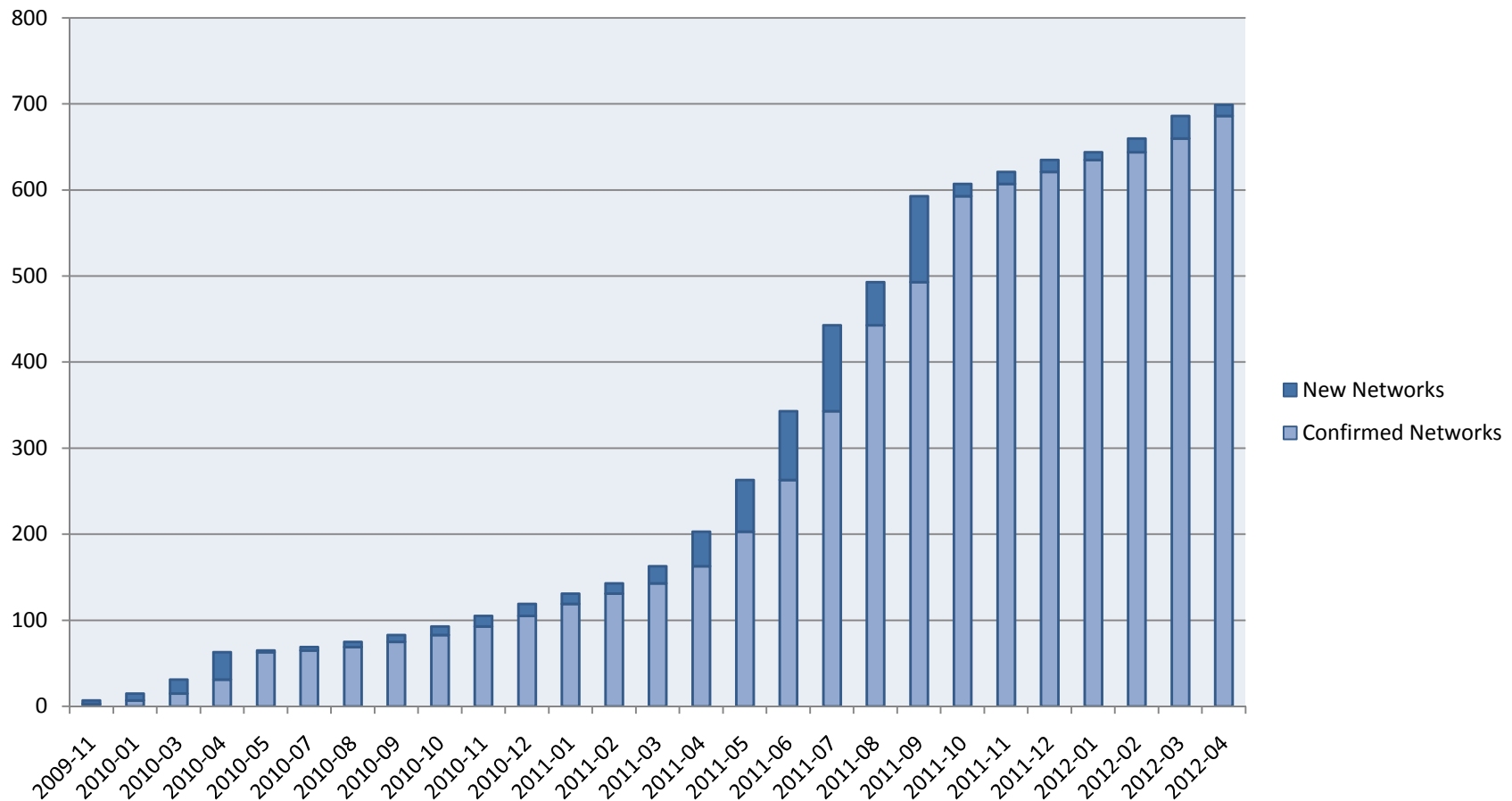


# Metrics: Network Discovery



(S//SI//REL)

(S//SI//REL) GSM/UMTS/LTE Networks Discovered in SIGINT



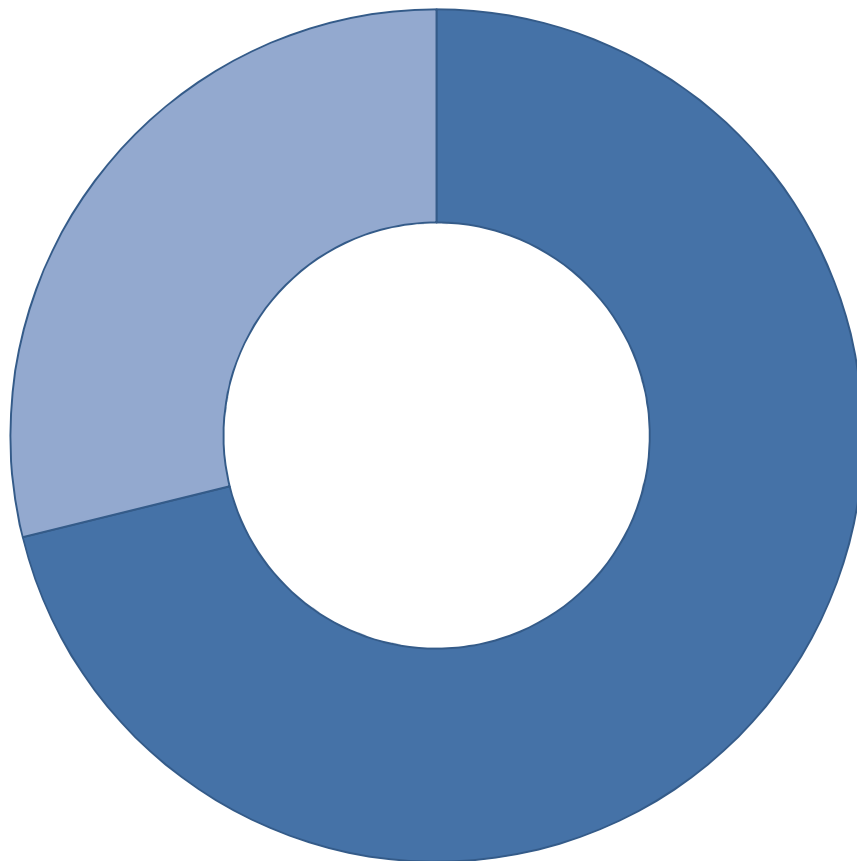


# Metrics: Network Discovery



(S//SI//REL)

(S//SI//REL) GSM/UMTS/LTE Network Coverage



- (S//SI//REL)
  - 701 confirmed
  - 985 estimated
  - 71%

(as of 15 May 2012)



# Network Coverage

(S//SI//REL)



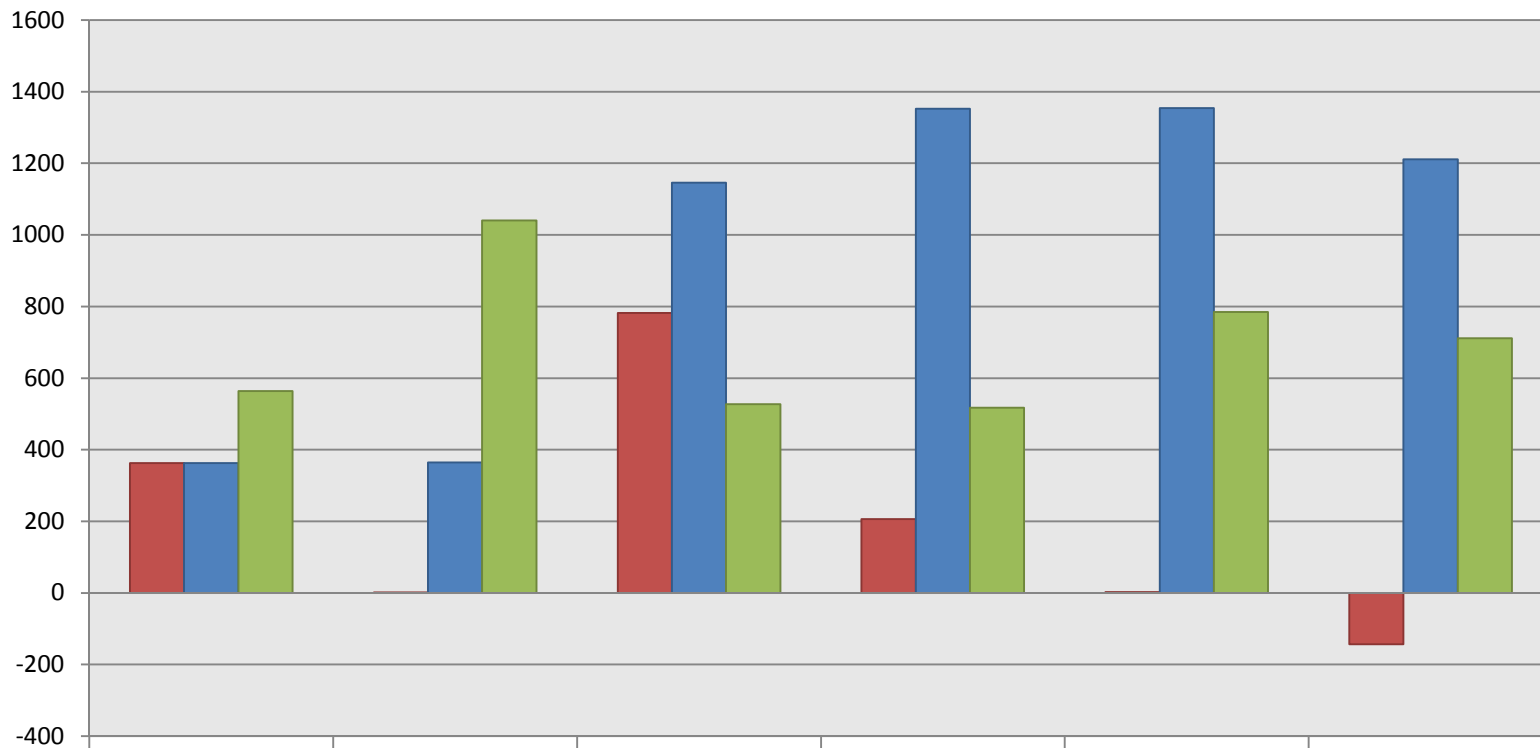


# Metrics: Tasking



(S//SI//REL)

## (S//SI//REL) Strong Selector Targeting



	2011-11	2011-12	2012-01	2012-02	2012-03	2012-04
Net change in tasking	363	1	782	206	2	-143
Total tasked	363	364	1146	1352	1354	1211
Extracted from IR.21s	564	1040	527	517	785	711

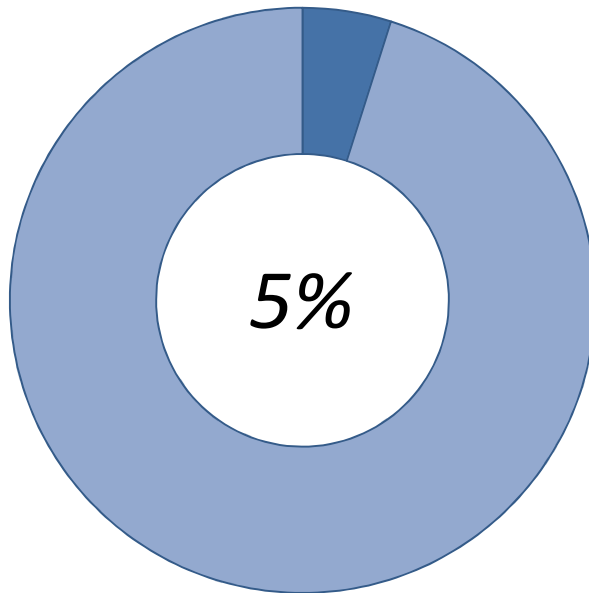


# RAEX Adoption in SIGINT



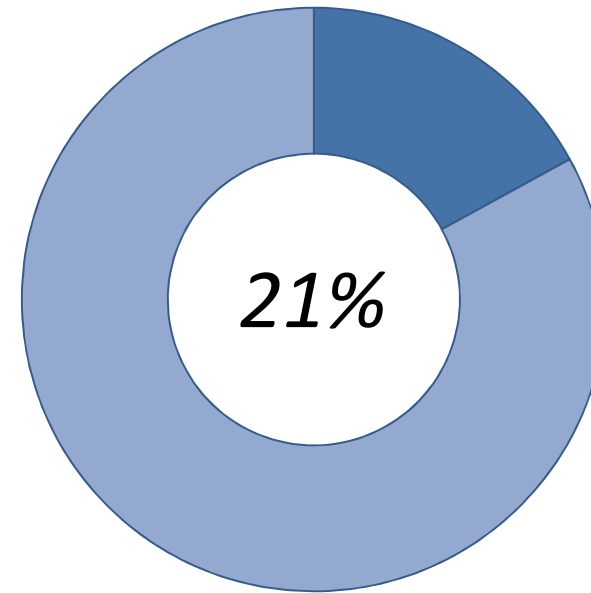
(S//SI//REL)

(S//SI//REL) What we've seen so far...



(S//SI//REL) 36/699 networks  
(Apr 2012; AURORAGOLD)

(TS//SI//REL) What we expect...



(TS//SI//REL) 202/985 networks  
(19 Apr 2012; 3/00/515656-12)





# Network Tradecraft Advancement Team (NTAT) 3G

## 2<sup>nd</sup> SCAMP at CSEC process

- Worked with CSEC H3 developers to implement IRASCIABLE RABBIT into OLYMPIA
- Developed 41 use cases
- Developed 10 new working aids
- Identified 3 new QFDs
- Research conducted on GRX operators over VPN (QFD: IRASCIABLE HARE)
- Progressed IR21 sharing and analysis
- Explored other GSMA Association for network intelligence
- Progressed signalling over IP analysis (QFD: BOLSHIE POSSUM)
- MNO EEI target template in development
- Identified training scenario
- Conducted real-world training scenario
- Tied together target analysis to network analysis process
- Use cases and working aids follow a layered template
- Research conducted on clearing house operators – identified key documentation and selectors
- Explored the usefulness of IR21 processing – decided against this
- Integrated TOYGRIPPE analysis into OLYMPIA
- Streamlined identification of VPNs of interest for crypt analysis

[http://\[REDACTED\]](http://[REDACTED])





TOP SECRET//COMINT//REL TO USA, FVEY



(S//REL TO USA, FVEY ) IR.21 – A Technology  
Warning Mechanism

SDC2010

[REDACTED]  
SSG4/T3C Technical Director

Derived From: NSA/CSSM I-52  
Dated: 20070108  
Declassify On: 20341201

TOP SECRET//COMINT//REL TO USA, FVEY





TOP SECRET//COMINT//REL TO USA, FVEY



# Classification

---

- ▶ This briefing is classified:
- ▶ **TOP SECRET//COMINT//REL TO USA, FVEY//**



TOP SECRET//COMINT//REL TO USA, FVEY



(U//FOUO) **Today's Agenda**

---

- ▶ (U) **Emerging Operating Model for Trends and Forecasting**
- ▶ (U) **Wireless Evolution Paths**
  
- ▶ (S//REL TO USA, FVEY) **Analytic Framework**
- ▶ **...and Process**
  
- ▶ (S//REL TO USA, FVEY) **Meet AURORAGOLD**
  
- ▶ (U) **An Invitation to Join – Your Use Cases...**
  - ▶ Includes Home Work Assignments...

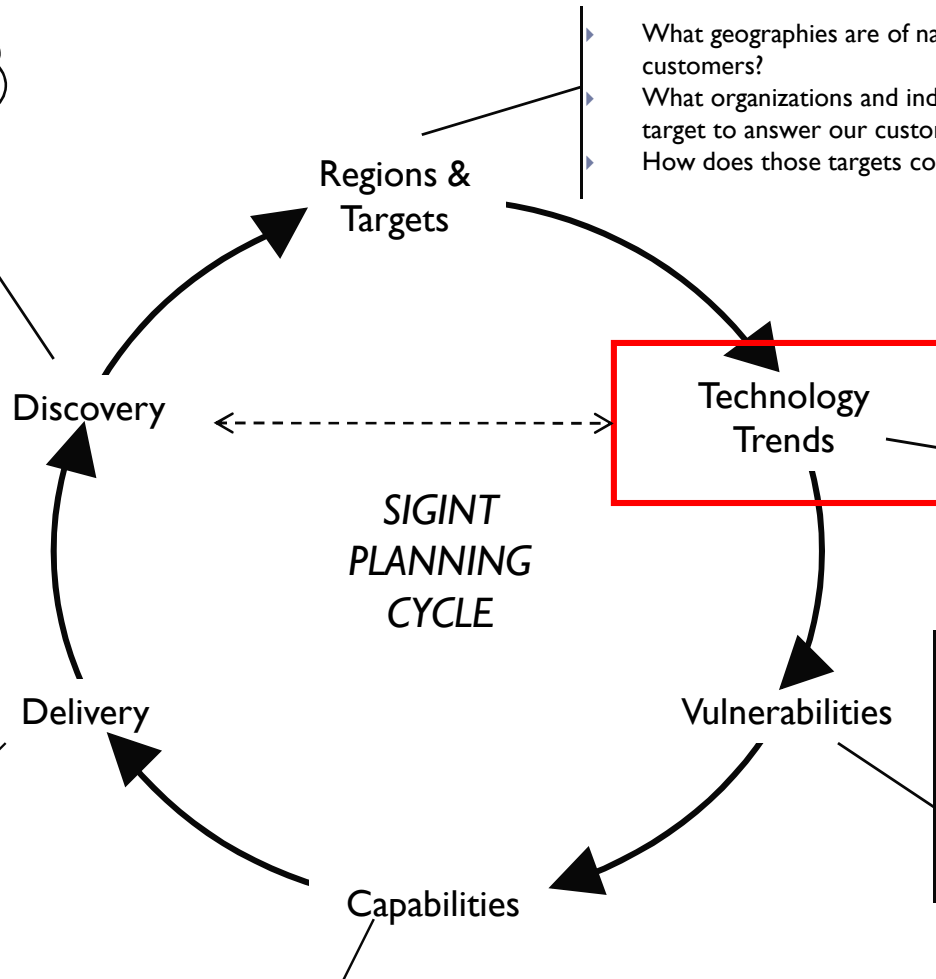




# (U//FOUO) Effective Forecasting: Geopolitical Regions and Targets

Discovery also critical

- ▶ How should discovery inform what targets/geographies we focus on next?
- ▶ How do we discover target adoption of a technology?



- ▶ What geographies are of national interest to our customers?
- ▶ What organizations and individuals must we target to answer our customers' questions?
- ▶ How does those targets communicate?

- ▶ How is technology evolving?
- ▶ How are technology and telecoms evolving in regions of interest?
- ▶ How do we expect targets to use emerging technologies?
- ▶ What is the SIGINT threat of these emerging technologies?

- ▶ What products/services do we produce for which customers?
- ▶ What is workforce makeup and how are they distributed?
- ▶ What role do partners play?

- ▶ What vulnerabilities are critical to current success (i.e. where are our risk areas)?
- ▶ How do we discover vulnerabilities?
- ▶ How do we introduce vulnerabilities where they do not yet exist?

- ▶ What capabilities do we need to develop to take advantage of technology vulnerabilities?
- ▶ What techniques do we deploy to take advantage of those vulnerabilities (e.g. CNE, supply chain, mid-point, etc.)
- ▶ What role does enabling, cooperative access, HUMINT, 2nd parties, etc. play in building those capabilities?



## (U) Two Types of Investigations

---

- ▶ (S//REL TO USA, FVEY) **Horizon Scanning**
    - ▶ Objective: Initial identification and assessment
    - ▶ All source research
    - ▶ Answer the question: Does this technology appear to be a large risk to the SIGINT system? Why or why not?
  
  - ▶ (S//REL TO USA, FVEY) **Deep Dive**
    - ▶ Objective: Cause a funding decision(s)
    - ▶ All source research; emphasis on geographic uptake trends; target uptake plans or vignettes.
    - ▶ Answer the question: Are SIGINT targets taking up this technology? How *fast*?
    - ▶ Implicitly contrast the above with the *cost and time* needed to remediate any SIGINT system shortfalls.
-



# (U) Trends and Forecasts: A Geo-temporal Tracking Problem

---

- ▶ (U) **Forecast:**
  - ▶ “An estimation of a Future Condition” ...
  - ▶ “To calculate or predict some future event or condition usually as a result of the analysis of available pertinent data” – Merriam Webster
  
- ▶ (U) **Trend:**
  - ▶ “To extend in a general direction; follow a general course”  
– Merriam Webster
  
- ▶ (U) **By necessity, a trend-line requires measurement of understood variables across time.**



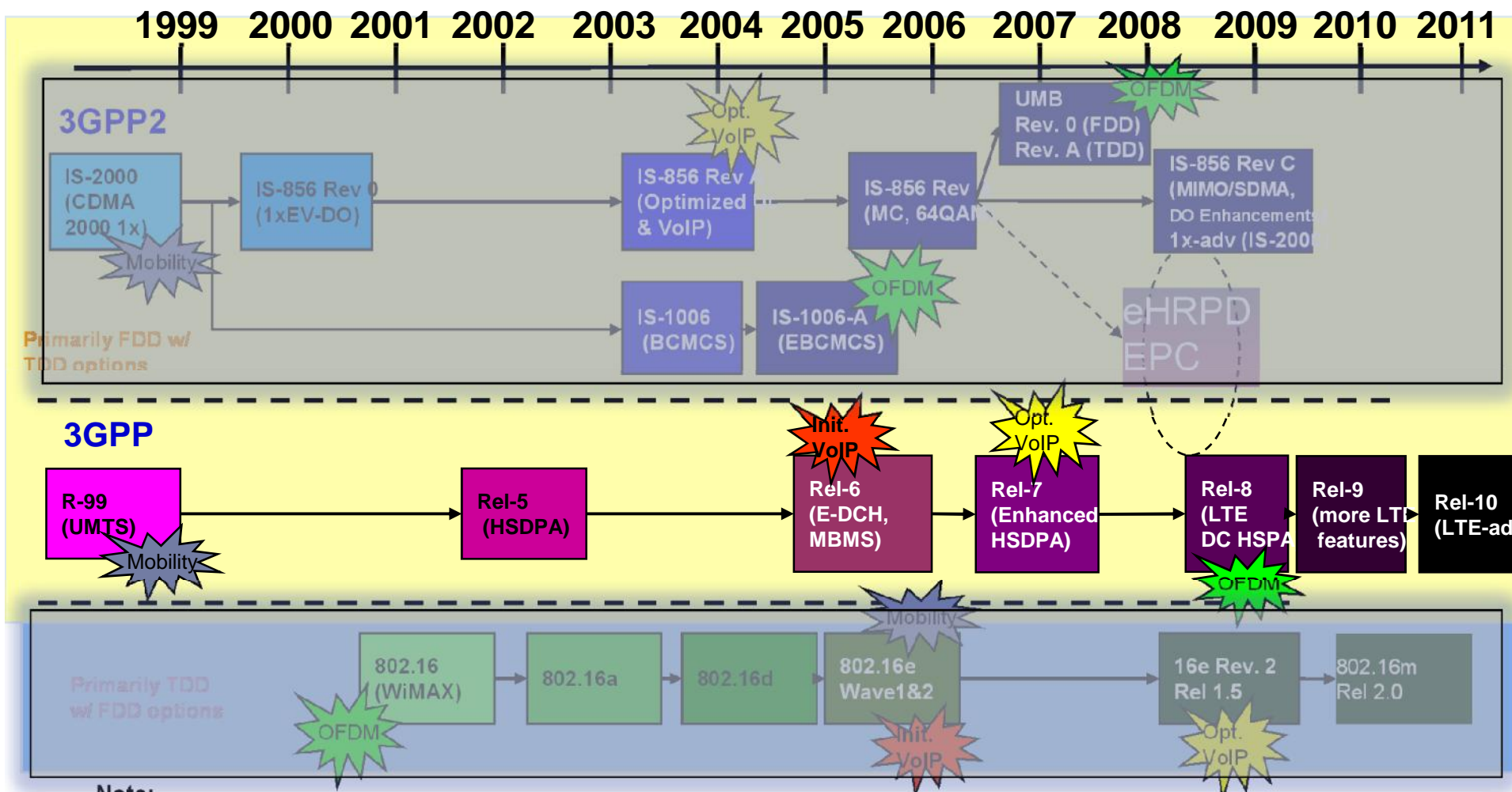
## (U) Roaming Agreements

---

- ▶ (U) Allow a mobile subscriber to use resources on a visited network
  - ▶ Each carrier's IR.21 is a technical document that:
    - ▶ Describes the operator itself in various ways
      - Location, business codes, etc.
    - ▶ Describes access to the IP network of the operator
      - DNS, IP addresses, ASN, etc.
    - ▶ Describes:
      - Radio Access Network: technology(ies) type(s)
      - Frequency(ies)
      - Telephony routing information (MSISDN ranges; E.212)
      - SCCP gateways (Point codes)
      - Mobile Application Part protocol in use
      - Hardware, software versions of certain network elements...
  
- ▶ (S//REL TO USA, FVEY) Hypothesis: We can identify and track a carrier's technical evolution with IR.21 and other data.



# (U) 3G Wireless Standards Evolution – Overview



**Note:**

- **Dates shown are standards completion dates** (or expected completion dates.)
- “Initial VoIP” not as spectrally efficient as “Optimized VoIP”.
- “Mobility” indicates when each particular standard supports mobility inter-operability between the terminal and BTS.

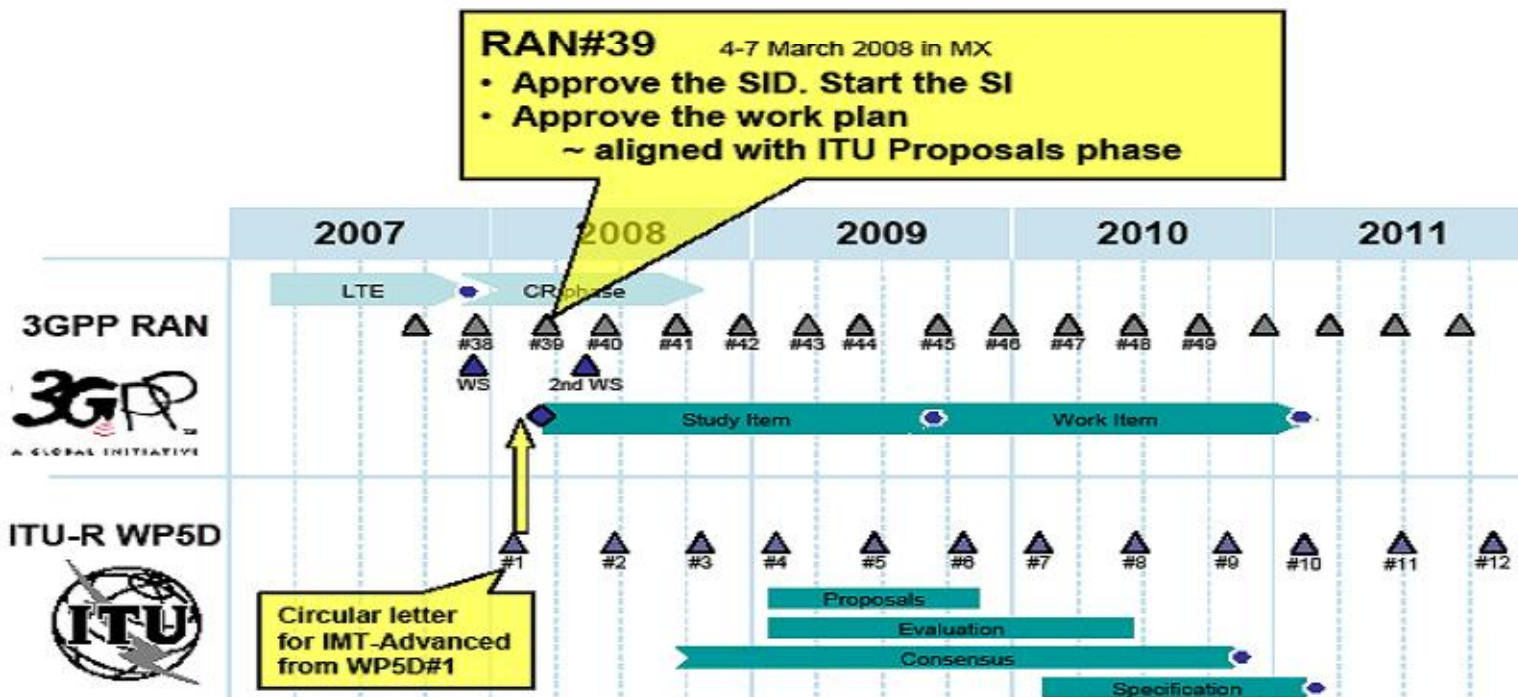




# (U) And What About 4G?

- ▶ (U) **IMT-adv** is an **ITU** led effort to set requirements for next gen. mobile networks
  - ▶ Just as ITU's IMT-2000 defined 3G, ITU's IMT-adv will define 4G

## Proposed 3GPP Work Plan





## (U) Framework for Analysis...

---

### ▶ (U) 3GPP: Defines technology migration paths.

#### ▶ “Releases” – A Clear Technology Roadmap

- 3G begins with Release 99
- Other releases: 04, 05, 06, 07, 08, 09, ....10, 11 (future)
  - See: [www.3gpp.org/ftp/Information/WORK\\_PLAN/Description\\_Releases/](http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/)
- Releases cover:
  - Access: GSM, EDGE, HSPA, LTE, LTE-Advanced, etc.
  - Core: GSM Core, Enhanced Packet Core...
  - Services: MS, etc.



### ▶ (U) GSMA: Defines carrier information exchange required to enable roaming

- Changes to IR.21 format warn of imminent technology roll-out
- An IR.21 is a GSMA-mandated document. IR.21 are exchanged between Wireless operators with roaming agreements, to the GSMA, and to certain clearing house operations.

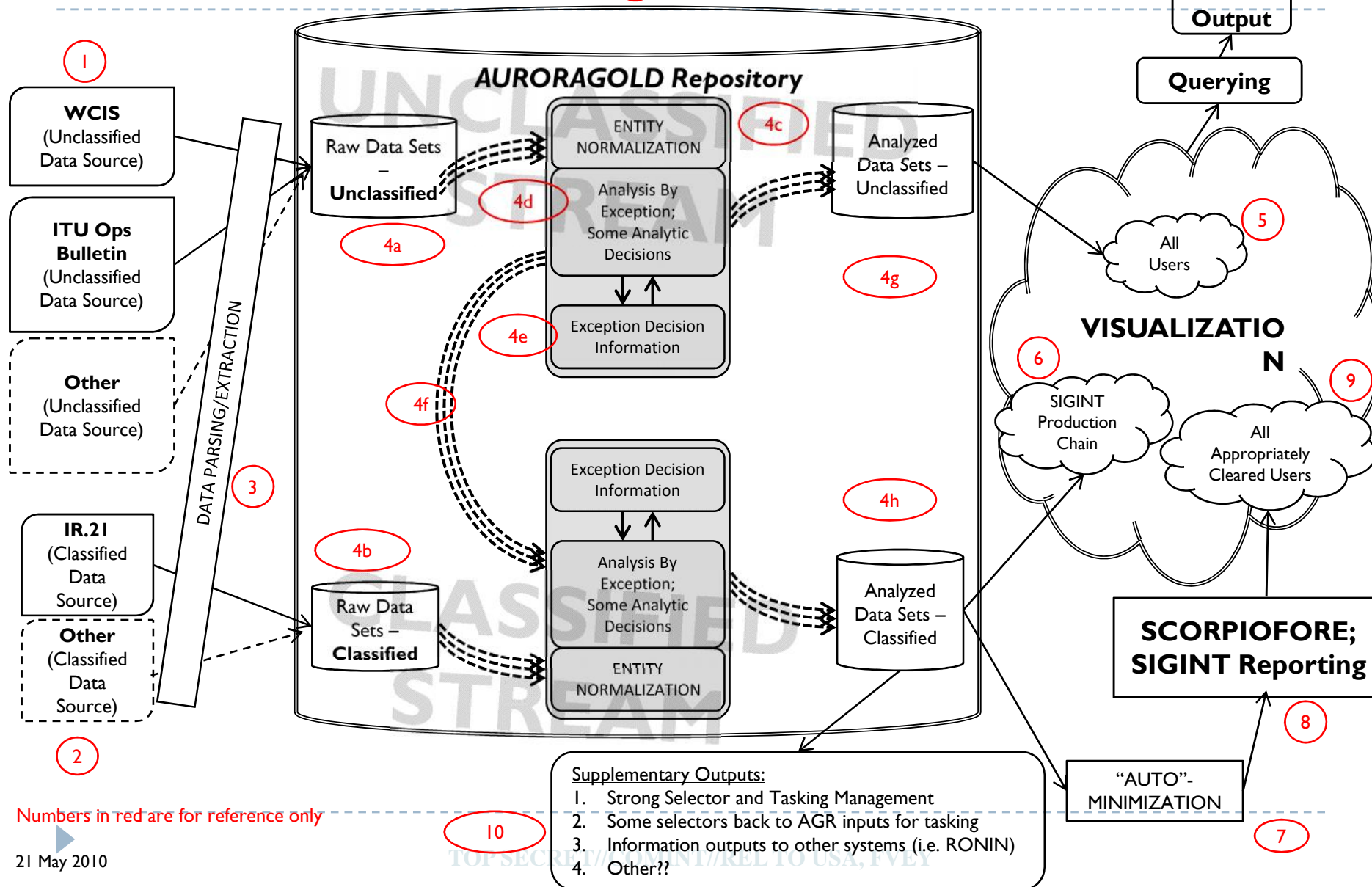


## (U) Analytic Process

- ▶ (S//REL TO USA, FVEY) **Data analysis process is to match information in IR.21, or elsewhere, against Releases in the Technology Roadmap**
  - Example: CAMEL Phase 4 (aka CAMEL4) as proxy for Release 5 deployment
  
- ▶ (S//REL TO USA, FVEY) **Analytic goals:**
  - ▶ Establish a date-time for a release deployment
  - ▶ Track releases at the per network level
  - ▶ Display status at the national, regional, hemispheric or global scale
  - ▶ Measure speed of adoption at each scale
  - ▶ Identify early and late adopter tendencies by network
  
- ▶ (S//REL TO USA, FVEY) **Deliverables:**
  - ▶ Adoption trends over time
  - ▶ Forecasts derived from trends and framework changes
  
- ▶ ▶ Formal reporting of data and conclusions – as a dataset



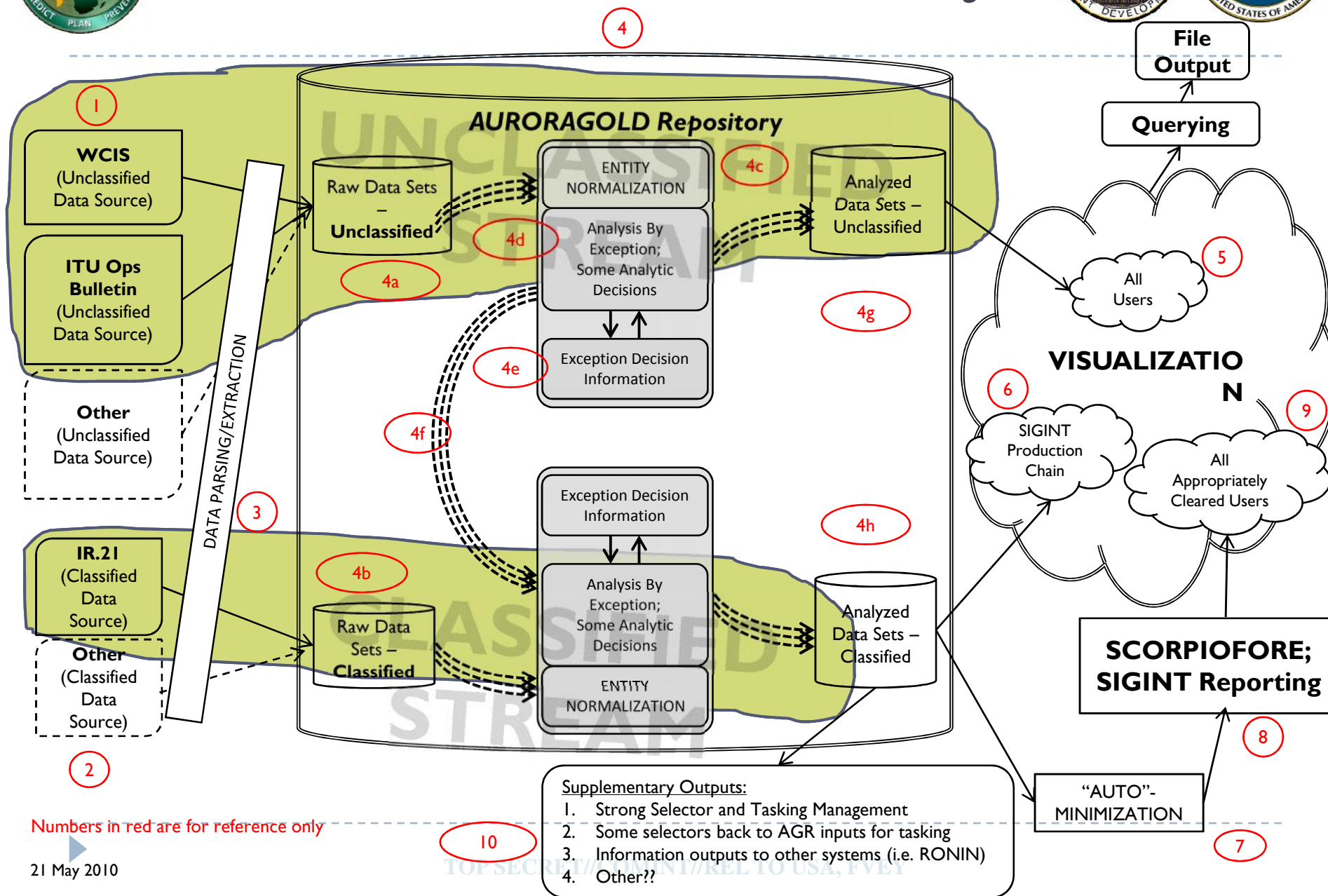
# (TS//SI//REL TO USA, FVEY) Data Flow and Process Overview







# What Is Done Today



Numbers in red are for reference only



TOP SECRET//COMINT//REL TO USA, FVEY

(S//REL TO USA, FVEY) **Information  
Delivery Vehicles – At NSA**



- ▶ (S//SI//REL TO USA, FVEY) **Mobile IP Information:**



- ▶ (S//SI//REL TO USA, FVEY) **Telephony and Provider information:**



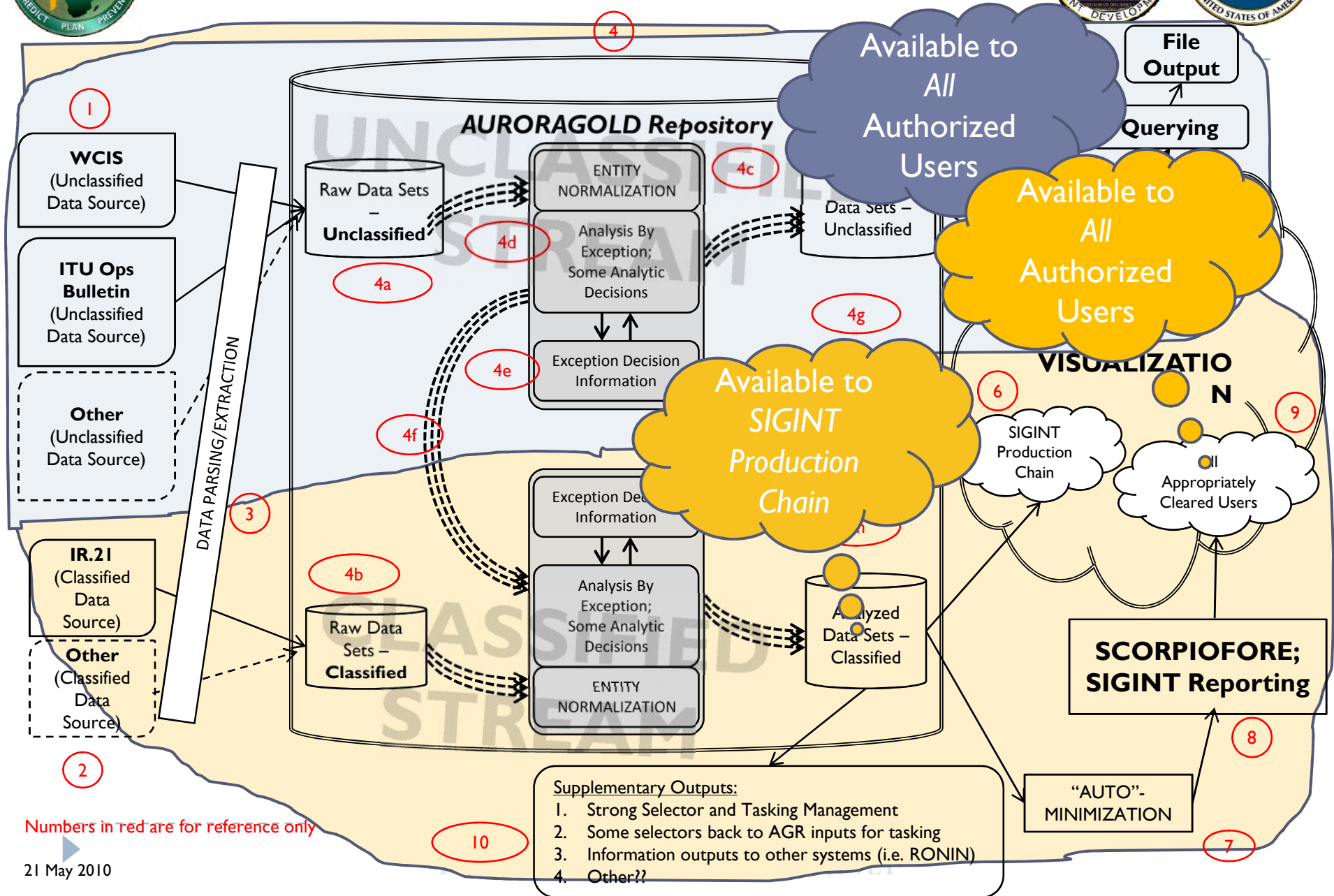
- ▶ (S//REL TO USA, FVEY) **Worldwide Wireless Market information:T3C**
  - packaged for WPMO consumption
    - Drives its portfolio investment planning process
    - Affects ~80% of the portfolio (2009), per customer.
- ▶ (U) **Various and sundry others ...**

TOP SECRET//COMINT//REL TO USA, FVEY





# Future Implementation



Numbers in red are for reference only



## (U) Information – Now What?

---

- ▶ (S//REL TO USA, FVEY) **Make the data useable**
  - ▶ Available in or out of the SIGINT production chain
  - ▶ Attach flows to value-adding chains and processes
  - ▶ Deliver as a data-set
  - ▶ Recognize other data sets exist and also are part of analytic processes (federation anybody?)
  
- ▶ (S//REL TO USA, FVEY) **Make the data traceable**
  - ▶ Includes auto-sourcing of data origin
  - ▶ Time-stamping
  
- ▶ (S//REL TO USA, FVEY) **T3C will do technology trending and warning...**
- ▶ (U) **Would your analytic processes benefit from this data set?**





## (U) Your Invitation to Join

---

- ▶ (U) **We are few; we welcome partnership.**
  - ▶ Can you help?
  - ▶ Do you have a better way?
  - ▶ Let's pull together!!
  
- ▶ (TS//SI//REL TO USA, FVEY) **We are preparing to measure the breadth of our access to IR.21 documents...**
  - ▶ **Goals:**
    - Do we cover all 3GPP networks?
    - Tweak access
    - Tweak selectors
  - ▶ **Indexer will provide PWID for all identified IR.21, after dedupe.**



## (U) What Are Your Use Cases?

---

- ▶ (S//REL TO USA, FVEY) This is your segment—to make the notetaker's job simpler please categorize your use case; describe impact:
  - ▶ A) IP Network
  - ▶ B) Call Control – Switched Voice
  - ▶ C) Hardware model and software version information
  
- Group Discussion....



---

▶ (U) Thank you for your time and contributions

▶ [REDACTED]

▶ [REDACTED]



# TOP SECRET STRAP1

TALIS Phase 2 Test & TTO Plan

SMO/00007CPO/4524/P02003/000/05

18 September 2009

## 3.6 A5/3 crypt attack proof-of-concept demonstrator

### 3.6.1 Scope

To successfully prosecute A5/3 enciphered GSM air-interface intercept requires changes to each part of the current A5/1 processing chain. This is a new requirement and has the covername of OPULENT PUP.

### 3.6.2 Requirements & Acceptance Criteria

RFC ST1823			
Identifier	CmR	Acceptance Criteria	Notes
S-SMP_CmR-xxxx	Trial A5/3 crypt attack hardware	Revalidated IA for OPULANT PUP RFC ST1823	

**(TS//SI//REL) Site Makes First-Ever Collect of High-Interest 4G Cellular Signal**

FROM: [REDACTED] and [REDACTED]  
RAINFALL (F78)  
Run Date: 02/23/2010

(TS//SI//REL) A collaborative effort between on-site collectors, engineers, and off-site contractors in mid-January 2010 allowed RAINFALL to make what is believed to be the first collection, by any known asset, of Time Division-Long Term Evolution (TD-LTE) 4G (fourth generation) cellular communications. Exploitation of this signal, an all-Internet Protocol successor to 2G and 3G cellular systems, is a very high priority for NSA and the Intelligence Community. The TD-LTE signal will enter the market in 2010 and become globally important by 2012.

(U) For full details, click [HERE](#).

(U//FOUO) **Note:** A valid PKI certificate with TK clearance is required to access the above article.

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



# TOP SECRET STRAP1

9 March 2011

DISCOVER ID 5100181

ANNEX A

Strategic Objective	Goal/Aim	Programme Outcomes	Target Capability deliveries for 2011/12
		Meet the Mobile Broadband challenge.	<ul style="list-style-type: none"><li>Scaling up the exploitation of handsets and Mobile Apps.</li></ul>
		Provide capability against Mobile encryption	<ul style="list-style-type: none"><li>WOLFRAMITE – Definition and prototyping of GSM A5/3 decryption (funding decision to be made (of the order of £4m) probably in 2Q of 11/12)</li></ul>

# TOP SECRET STRAP1

9 March 2011

DISCOVER ID 5100181

ANNEX A

Strategic Objective	Goal/Aim	Programme Outcomes	Target Capability deliveries for 2011/12
		Respond to the roll out of the next Mobile OTA encryption standard for GSM (A5/3) by developing an attack with NSA, and for which there is significant SIA interest.	WOLFRAMITE R&D and definition.