

CRYPTOME

19 May 2014

Ryan Devereaux, The Intercept, released on 19 May 2014 these 12 pages of NSA documents obtained by Edward Snowden.

Related article:

<https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/>

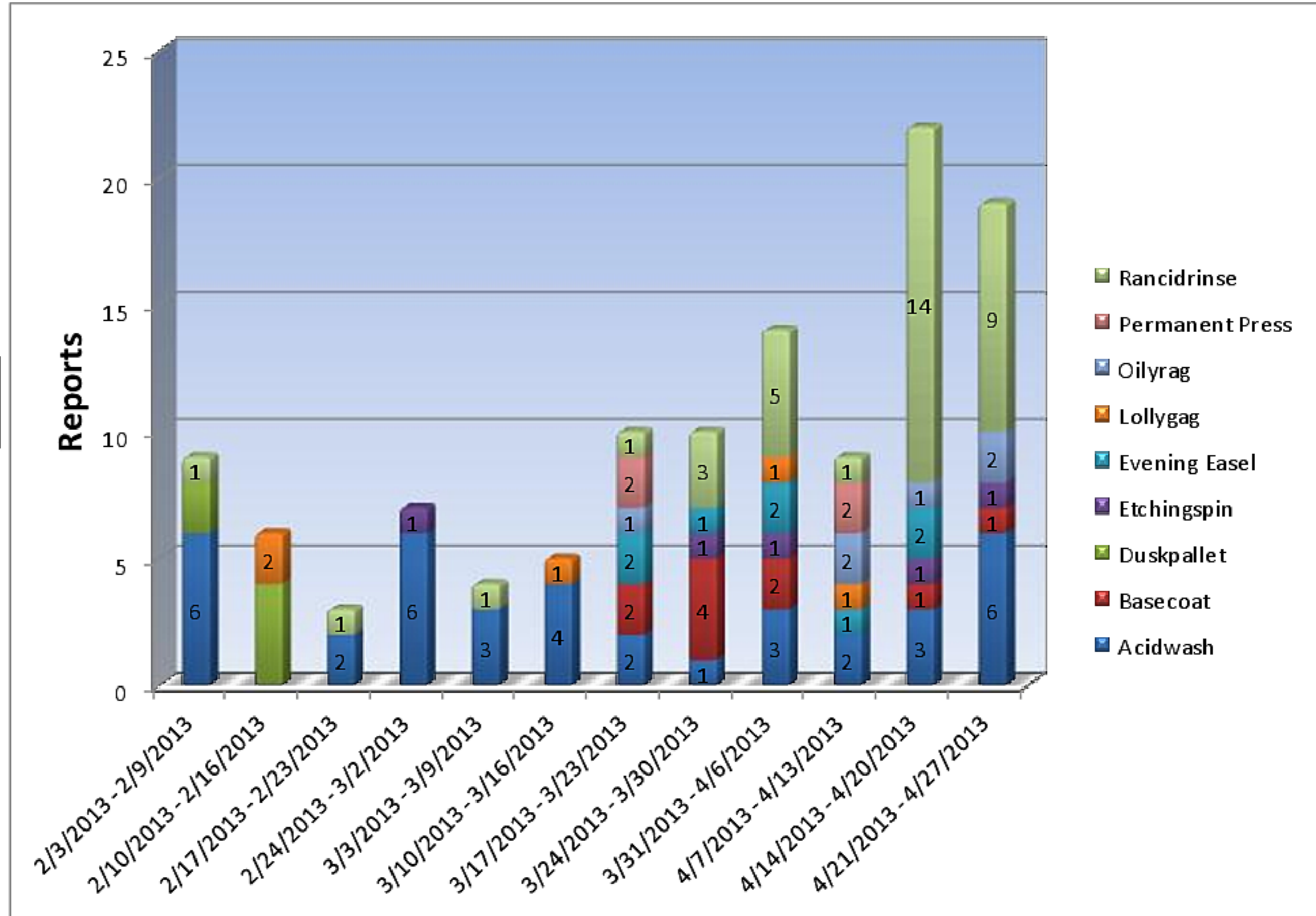


(U//FOUO) MYSTIC Reporting (Excluding Scalawag)

Talking Points:

. Approx. 10 – 15
SIGINT Reports per
week from Mystic
sites other than
Scalawag

[REDACTED]
from Mystic sites
other than Scalawag,
Oilyrag, and
Acidwash for the
week of April 21st –
April 27th



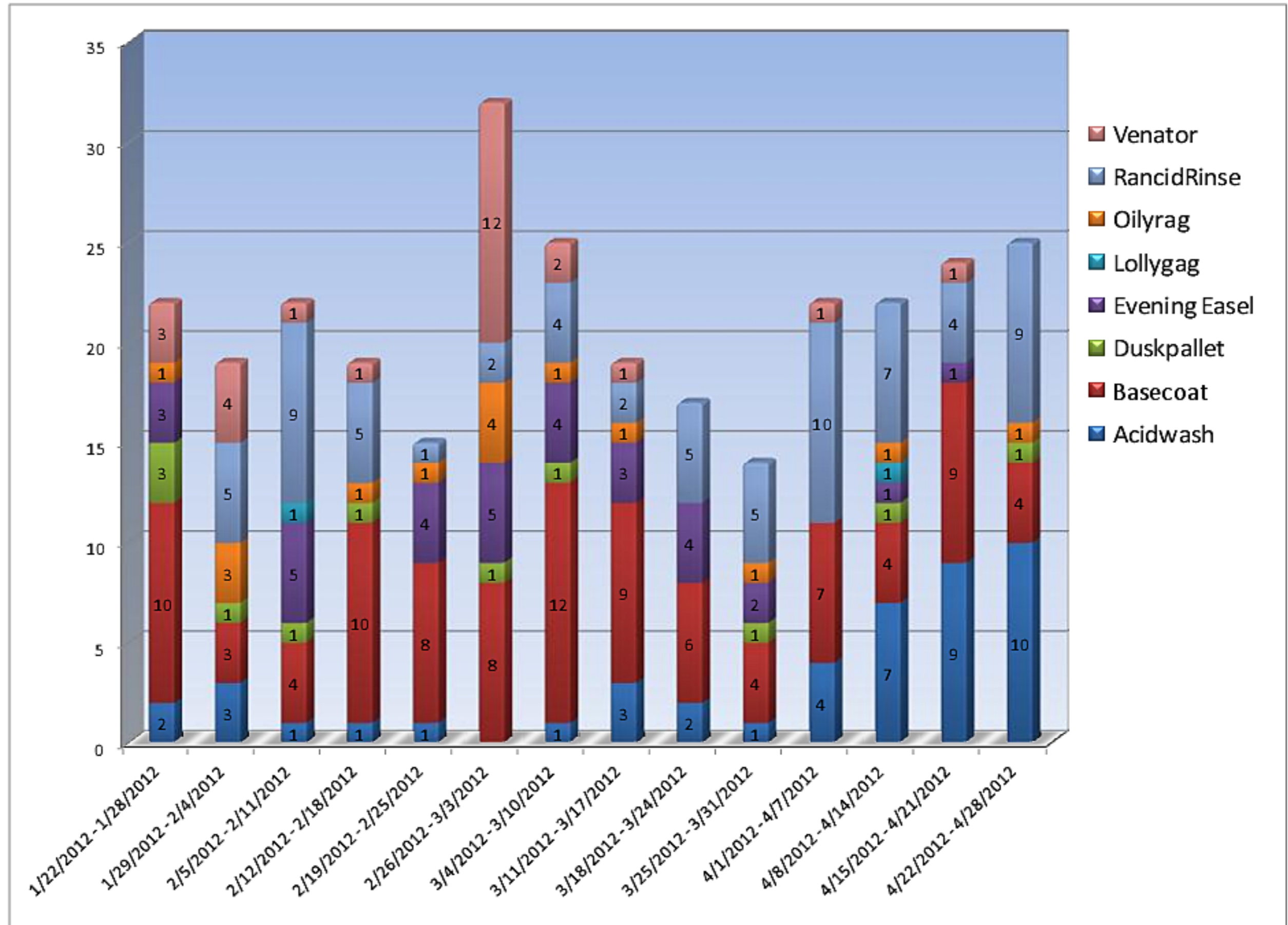


(U//FOUO) MYSTIC Reporting (Excluding SCALAWAG)

Talking Points:

Approx. 15 – 20
SIGINT Reports per
week from MYSTIC
sites other than
SCALAWAG

[REDACTED]
from MYSTIC sites
other than
SCALAWAG,
ACIDWASH, and
OILYRAG for the
week of April 22nd –
April 28th



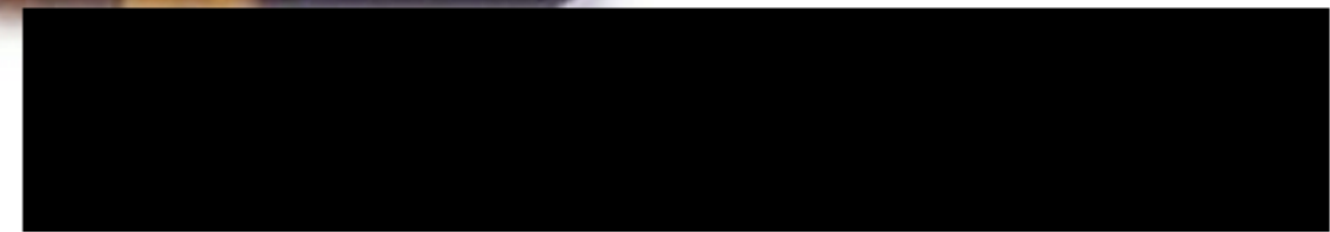


(U//FOUO)

MYSTIC



(U//FOUO) BRIEFER:



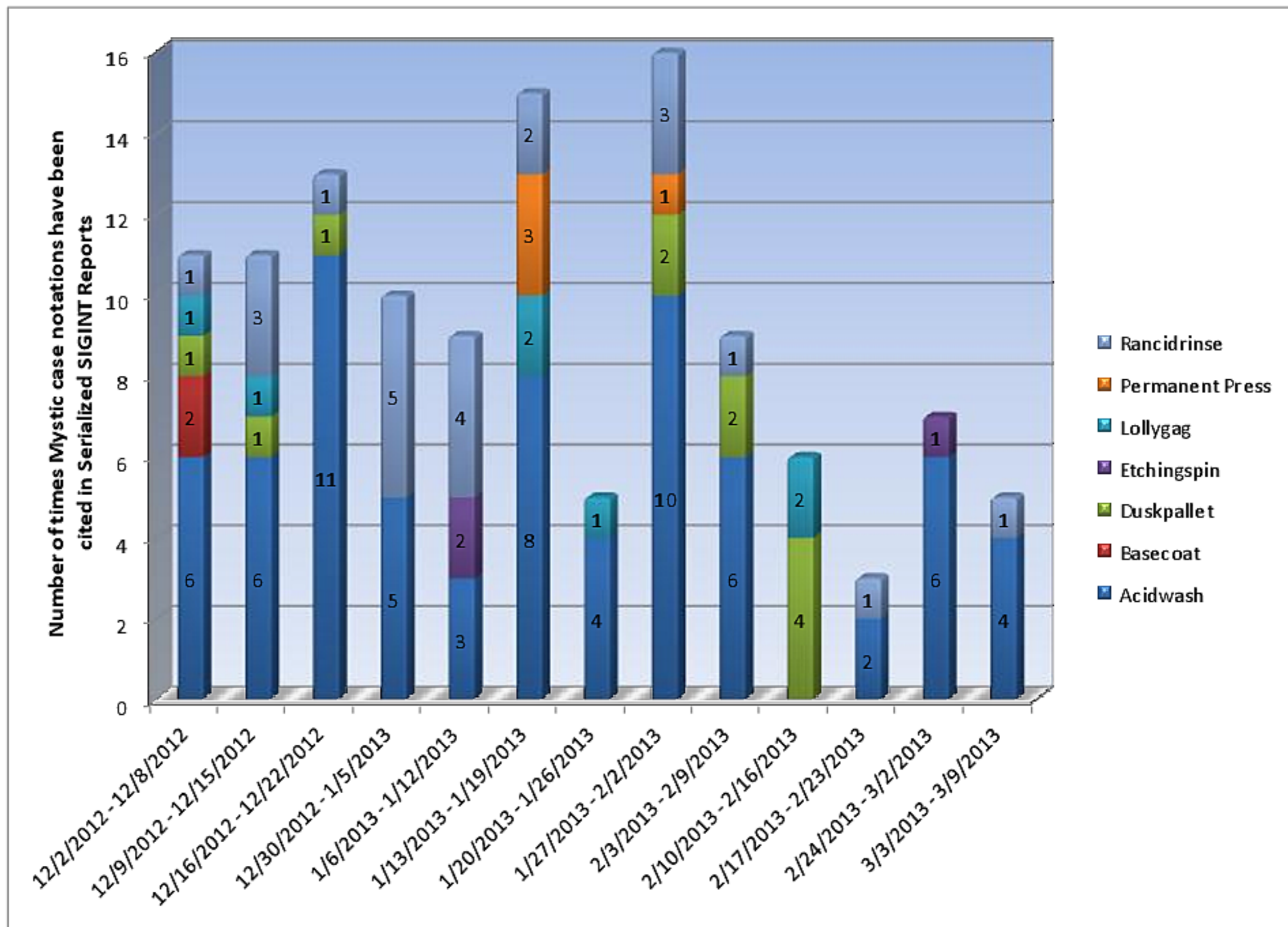


(U//FOUO) MYSTIC Reporting (Excluding SCALAWAG)

Talking Points:

Approx. 10 – 15
SIGINT Reports per
week from MYSTIC
sites other than
SCALAWAG

from MYSTIC sites
other than
SCALAWAG,
OILYRAG, and
ACIDWASH for the
week of March 3rd –
March 9th





(U) WHAT'S NEW

➤ US-3310A1/A2/BASECOAT (Bahamas) reactivated mid-March. Five reports issued by end of March, four sole source.

2/00/501291-13

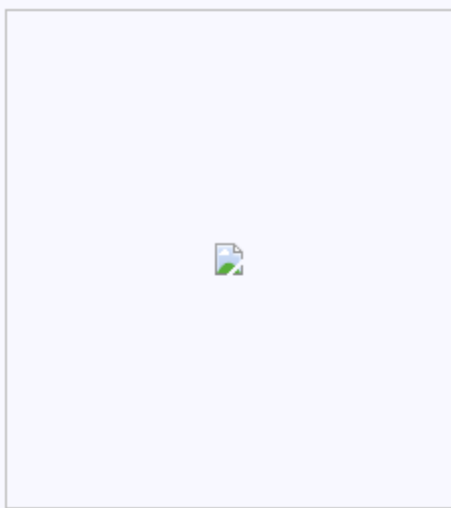
(S//SI//REL TO USA, FVEY) Additionally, ██████ arranged Mexico-to-United States marijuana shipments in late March. ██████ informed ██████ that it was possible to send up to 90 pounds of marijuana via the United States Postal Service without being charged with a felony, and that ██████ had conducted this sort of shipment successfully several times already. ██████ expected the marijuana to be inserted in packages after they had been inspected by United States customs officials in Mexico. ██████ believed that unspecified individuals removed the customs inspection seal, inserted the narcotics, and reapplied the seal.

(U) Project Description

(S//SI//REL TO USA, FVEY) The Special Source Operations (SSO) Project provides management oversight and logistical support to the Special Source Access programs. These resources are used to provide cross-program management services to drive efficiencies within the Special Source Access Expenditure Center (EC). Responsibilities include general management, training, and travel. This Project supports the RAMPART-I program in [REDACTED] and the RAMPART-X program in [REDACTED]. It also supports the MYSTIC Program Office, which leverages partner-enabled accesses against Global System for Mobile Communications (GSM) and other cellular and Public Switched Telephone Networks (PSTNs). It supports target technology development through comprehensive and definitive description of foreign targets' current and future use of telecommunications and computer systems. Additionally, this Project sustains efforts to add, enhance, and support Next-Generation Wireless (NGW) capabilities across Special Source Accesses, and efforts to address critical target capability gaps. This Project contains the Special Source Staff Operations Sub-Project.

(U) Base resources in this project are used to:

- (U//FOUO) Provide travel, training, equipment and general supplies for the Special Source Access front office.
- (TS//SI//REL TO USA, FVEY) Provides initial and emerging access to high-priority SIGINT targets against new requirements, provide management and technical engineering services to analyze and maintain data flow, provide program metrics, and manage allocation of tasks and schedules for SSO collection sources.
- (S//SI//REL TO USA, FVEY) Provide contracted services for NGW core network exploitation capabilities to deploy core network exploitation capabilities to collection sites in [REDACTED], Caribbean, Kenya, the Philippines, and Mexico.
- (C//REL TO USA, FVEY) Purchase classified SIGINT processing equipment, associated upgrades, and life-cycle support.
- (TS//SI//NF) Sustain MYSTIC capabilities to provide comprehensive metadata access and content against targeted communications in [REDACTED], Kenya, Caribbean, Mexico, and the Philippines. Provide new PSTN collection capability in [REDACTED] on their international links to [REDACTED] and [REDACTED]. Capabilities will offer near-real time, complete access to the additional target country's GSM network(s), and provide for retrospective tasking and near-real-time access/delivery of metadata as required. Activities previously provided by Overseas Contingency Operations (OCO) resources are now requested in the base submission.



MYSTIC

YEAR ESTABLISHED	(U) 2009
DESCRIPTION	(TS//SI//NF) MYSTIC is an SSO program for embedded collection systems overtly installed on target networks, predominantly for the collection and processing of wireless/mobile communications networks. The overt purpose is for legitimate commercial services for the Telco's themselves; our covert mission is the provision of SIGINT.
INTELLIGENCE VALUE	
MAJOR TARGETS	(TS//SI//NF) These systems directly support ██████████ ██████████ in their ██████████ Counter Terrorism, Counter Narcotics, and International Crime missions.
MAJOR BENEFACTORS & USERS OF INFORMATION	(TS//SI//NF) The MYSTIC program encompasses a number of subprograms, which are variously sponsored by NCSC, DEA, and CIA.

5	(TS//SI//NF) Plan for MYSTIC accesses against projected new mission requirements (i.e. 3G and 4G technologies, Voice data, etc.) (MOD)	3.1, 3.3
---	--	----------

- Other CIA sponsored sites:
- 5. DUSKPALLET - US-3270/DA - Kenyan GSM
 - 6. EVENINGEASEL (US-3411A/4F) Mexican Wireless

B) (TS//SI//REL TO USA, FVEY) ██████████ Sponsored

- * Known as SOMALGET sites with common US-3310-XX, PDDG ZD
- 1. BASECOAT - US-3310A Bahamas A-link GSM
 - o Includes sites US-3310A1 and US-3310A2

(U) DEA - The "Other" Warfighter

FROM: [REDACTED]
DEA Account Manager (S112)
Run Date: 04/20/2004

(U//FOUO) When you think about our top national security threats, chances are that terrorism and military conflict come quickly to mind - and for good reason. But how many of us list illegal narcotics among the top threats to our society? Our national leadership recognized the seriousness this problem poses and declared a war on drugs two decades ago. This "war" has all the risks, excitement, and dangers of conventional warfare, and the stakes are equally high.

(U//FOUO) We are all aware that the Drug Enforcement Administration (DEA) is leading our nation's counternarcotics (CN) efforts. But many are not aware that from the start NSA has been at the forefront of Intelligence Community (IC) support to this seemingly unconventional DOD mission. The novel collection and analysis techniques NSA developed and refined against these criminal hard targets have not only resulted in major successes in the war on drugs, but they have also proven invaluable to other critical SIGINT missions, particularly counterterrorism, sometimes blurring the lines between the two missions.

(C) DEA has close relationships with foreign government counterparts and vetted foreign partners. The results of this team approach regularly make the headlines in the form of major drug busts and arrests. Less known is the critical supporting role that NSA continues to play in key DEA operations to disrupt the flow of narcotics to our country and thwart other, related crimes. DEA, however, recognizes the unique access and sole source information NSA provides and coordinates major cases with the S2F/ICN Product Line.

(C) As a result, both agencies enjoy a vibrant two-way information sharing relationship that enhances their common mission. Processes have been carefully established to exchange lead (foreign intelligence) information while protecting NSA equities. The Customer Relationships Directorate (S1), the Data Acquisition Directorate (S3), and MRSOC work with the S2F/ICN office as an integrated team to realize these mission successes.

(S//SI) One of those successes: Based on SCS (US-966L) intercept, S2F/ICN issued an OPS IMMEDIATE report on 30 March 2004 on the exact whereabouts of Colombian narcotics trafficker Gonzalo Hinojosa, an evasive and brutal international fugitive wanted for murder, drug trafficking, and money laundering. S2F had the foresight to include a tearline to share the actionable intelligence with Panamanian partners. With a short window for action, NSA's [REDACTED] worked through the Joint Interagency Task Force (JITF) - South to immediately forward the information to DEA/Panama. DEA/Panama in turn alerted the Panamanian authorities who quickly located and apprehended Hinojosa, without knowing the information came from NSA SIGINT. As Chief [REDACTED] noted, this is an excellent example of "outcome-oriented collaboration."

(U//FOUO) To learn more about NSA support to the "other" warfighter, DEA, visit the International Crime and Narcotics (S2F) [website](#).

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 ([DL sid_comms](#))."

Information Owner: [REDACTED] S0121, [REDACTED] ([email](#))

Page Publisher: [REDACTED] S0121, [REDACTED] ([email](#))

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

computer center



(S//SI//REL) Intro: Here in S2F, we've had great success using systems that buffer full-take audio collection for a nominal 30 days -- these systems have led to real breakthroughs in target discovery -- and we wanted to alert other analysts to their potential. Collectors: please take note of how beneficial these types of collectors can be to

analysts, as compared to more traditional models.

(S//SI//REL) SOMALGET is a family of collection systems which greatly facilitate and make possible remarkable new ways of performing both target development¹ and target discovery.² Significant analytic breakthroughs and successes in both areas have been made by SID analysts in the two countries where SOMALGET accesses currently exist (i.e., [REDACTED] and the Bahamas).

(U) How It Works:

(S//SI//REL) SOMALGET collection systems **forward full-take metadata in real time and buffer full-take audio for nominally 30 days.**³ It makes possible the selection of audio content against the buffered data after the fact, in near real-time, or up to 30 days later. This ability is dubbed "*retrospective retrieval*." The power of retrospective retrieval in facilitating target development or discovery lies in its ability to permit the analyst to selectively retrieve audio content and immediately validate his/her tentative analytic conclusions derived from metadata.

- (TS//SI//REL) SOMALGET access to Bahamian GSM communications has led to the **discovery of international narcotics traffickers and special-interest alien smugglers.** This access -- together with our use of methods that take advantage of targets' behavioral patterns⁴ -- have allowed our S2F analysts to gain a firm understanding of the targets' activities even when these contacts occurred prior to their discovery.

(U) More to Come?

(S//SI//REL) These successes, which depend on access to buffered audio files that may be associated with selectors not tasked to the collection asset in question, **argue in favor of a collection methodology for telephony that may be viewed as analogous to [XKEYSCORE](#).** That is, we buffer certain calls that **MAY** be of foreign intelligence value for a sufficient period to permit a well-informed decision on whether to retrieve and return specific audio content. With proper engineering and coordination, there is little reason this capability cannot expand to other accesses (besides [REDACTED] and the Bahamas), provided compatible hardware and interfaces are developed and deployed.⁵

(U) Notes:

1. (U) Target development = the process by which an analyst can **extend his/her knowledge of a known target** by observing elements of metadata that relate to that target.
2. (U) Target discovery = the process whereby an analyst can **discover targets by observing metadata as it relates to behaviors** characteristic of his/her target set, regardless of whether or not the newly discovered selectors are related to known targets.
3. (S//SI//REL) The nominal "30 days storage" actually varies depending upon on space, power, and observed activity levels.
4. (TS//SI//REL) Observing that targets tend to use prepaid calling cards in an attempt to mask the destination of telephone calls, S2F focused on mobile identifiers in number ranges that represent newly activated accounts. We have also used SMS text messages to identify and retrieve audio of interest.
5. (S//SI//REL) Storage capacity is directly related to the amount of disk storage that can be deployed. When deployed against entire networks, as SOMALGET is, the back-end database and processing required for interactive search and retrieval of cuts also requires enterprise-class data warehousing and high-performance processing to manage the vast amount of data captured. Currently this warehouse dynamically manages roughly 5 billion call events, with the capacity to expand well beyond our current target communications. This retrospective retrieval infrastructure is web based and is already in place. As noted, with proper engineering and coordination, there is little reason this capability cannot expand to other accesses, provided compatible hardware and interfaces are developed and deployed.

BASECOAT	(TS//SI//NF) MYSTIC access; Bahamas A-link GSM. DEA access under LI that collects Counter-Narcotic (CN) targets. There are two sites located in the Bahamas. It is currently being used as a test bed for system deployments, capabilities, and improvements.
	(TS//SI//NF) NCSC covername for MYSTIC access provider
DUSKPALLET	(TS//SI//NF) MYSTIC access that collects Kenya GSM (DNR). Collection is on the Abis link and brings back GSM metadata with the potential for content at a later date. Similar to LAUNDROMAT accesses
EVENINGEASEL	(TS//SI//NF) SIMILAR to MYSTIC'S LAUDROMAT accesses. Pending access. Will collect Mexico GSM for CN targets. Site will be in Mexico.
GSM	Groupe Speciale Mobile or Global System for Mobile communications. It is the most widely proliferated digital cellular technology in the world today.
LI	Lawful Intercept
LOCKSTOCK	(U//FOUO) An eight year/\$51M Time & Material contract with General Dynamics, located in Annapolis Junction, MD, for the support of the LOCKSTOCK collection system used by MYSTIC and RAM-M. COR is currently [REDACTED]. Processes all MYSTIC data and data for other NSA accesses.
SOMALGET	(TS//SI//NF) SOMALGET- UMBRELLA term for systems provided by [REDACTED] (NCSC). Currently comprised of the SCALAWAG, OILYRAG, and LOLLYGAG collection systems in [REDACTED] and BASECOAT in the Bahamas. Processes over 100 million call events per day. The overt mission of for SOMALGET is under the Lawful Intercept (LI) auspices via DEA accesses. Host countries are not aware of NSA's SIGINT collection using these systems.
VENATOR	(TS//SI//NF) MYSTIC access via DSD asset in a Philippine provider site. Collects Philippine GSM, Short Message Service (SMS) and Call Detail Records. Will soon become a source of lucrative intelligence for terrorist activities in Southern Philippines.