ARTIFICE (TS//SI/NF) Covername for one of SSO's corporate partners

BIGBIRD (TS//SI//NF) A cable modernization effort, which began in 2004 to support the theme of a more focused, agile collection, a more cost-effective cover, and access to new higher priority cable systems. As part of the FAIRVIEW/SSO broad access, focused collection strategy, the BIGBIRD effort provided the program with significant additional access to targets on selected undersea cable systems, an automated remote survey capability, and a modernized collection and processing suite for exploiting this new access. The enclosed proposal for continued cable modernization, entitled POORWILL, will specifically focus on providing increased DNR access capacity and processing across all existing cable sites. Additionally, the proposed effort includes increased processing capacity at the Program's centralized processing facility - PINECONE.

BLACKBELT (T//SI//NF) FAIRVIEW Access

CASE NOTATION (S//SI//REL) An alphanumeric value that identifies the intercepted link being processed.

CADENCE C//SI) CADENCE is a DNI tasking tool. The CADENCE system fully automates the Front-End Dictionary Management process within Operations. Utilizing CADENCE, dictionary managers as well as target analysts are able to submit, review, and forward dictionary updates electronically. Receipts for these requests are automatically generated, statistics compiled and reported, and approved updates maintained in a database containing historical information for the DDO review of "USSID-18" compliance. Finally, CADENCE provides a transparent interface to BLACKNIGHT/SHIPMASTER, COURIERSKILL, and other site dictionaries.

CDR (TS//SI//NF) Call Detail Records (or Telephony Metadata) include comprehensive communications routing information, specifically, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, Mobile Subscriber Integrated Services Digital Network Number (MSISDN), International Mobile station Equipment Identity (IMEI) number, also trunk identifier, telephone calling card numbers, and the time and duration of call. Telephony metadata does NOT include substantive content of any communication, or the name, address, or financial information about a subscriber or customer. (Source: BR FISA End-to-End Report Glossary, dated 29 June 2009 and ADET/SV BR FISA Training Glossary on eCampus dated Sept 2009)

CNCI Comprehensive National Cybersecurity Initiative

COURIERSKILL (S//SI//REL) COURIERSKILL is a project under the THEORYMASTER program. It provides high performance content Filtering and Selection (F&S) capabilities to meet the current and future needs of Data Network Intelligence. COURIERSKILL also provides content F&S services for the WEALTHYCLUSTER 2.0 system. It is designed to replace the legacy BLACKNIGHT system.

CLIFFSIDE (TS//SI//NF) A FAIRVIEW site

CS (TS//SI//NF) CLIFFSIDE-A FAIRVIEW site

DISHFIRE (S//REL) DISHFIRE is a Short Message Service (SMS) storage and retrieval application developed by the Target Development Services (TAC/TDS) in response to formal requirements from the Counter Terrorism Office, and coordinated with the Rebuilding Analysis Center. DishFire offers retrieval, viewing, and some manipulation of SMS messages passed through various worldwide networks. As of September 2007, an Analyst Advisory Board (AAB) has been established to provide S2 Offices with insight into and an opportunity to comment on requirements levied on the DISHFIRE system.

DNI (U//FOUO) Digital Network Intelligence-is an analytic term, replacing C2C (Computer-to-Computer), referring to SIGINT derived from the 'digital network.' The term 'digital network' is commonly identified today with the Internet, but for the purposes of SIGINT includes both the Public Internet as well as private digital networks.
DNR (S//SI//REL) Dialed Number Recognition-The process of extracting dialed telephone numbers from the transmitted information present in a telephone signaling system. The dialed numbers are looked up in a "directory", which contains the phone numbers of persons from whom an analyst might gain intelligence information. If the extracted number "hits" in the directory, the associated conversation is recorded.

FAA FISA Amendment Actis an Act of Congress to amend the Foreign Intelligence Surveillance Act (FISA) of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes. Based on discussions by a cross-section of NSA experts from across SID, Oversight and Compliance and Office of the General Counsel, the following guidelines are provided to aid production elements in understanding and complying with the letter, spirit and intent of the procedures associated with FISA collection under the Protect America Act (PAA) and FISA Amendments Act. Under FISA authority, analysts are required to verify the foreignness of their target and confirm that the target is appropriate for tasking under PAA and FAA Certifications prior to actually tasking any selectors. Following that, analysts are required to verify the foreignness and nature of the target routinely once data begins to flow.
FAA702 FAA Section 702 (certain non-USPs reasonably believed to be located overseas)

FAA 702 Collection/Targeting:
U. S. persons may NOT be targeted under FAA Section 702.
Persons in the US may NOT be targeted under FAA Section 702.
Accounts used, shared or in any way accessed by USPs or persons in the US may NOT be targeted or remain on target under FAA Section 702. This applies even if the intended targeted user of the selector remains otherwise a non-USP reasonably believed located outside the US.

FAA 702 Collection/Querying:

Update While the FAA 702 minimization procedures approved on 3 October 2011 now allow for use of certain United States person names and identifiers as query terms when reviewing collected FAA 702 data, analysts may NOT/NOT implement any USP queries until an effective oversight process has been developed by NSA and agreed to by DOJ/ODNI. Until further notice, analysts must ensure that database queries, including federated queries, of any USP selection terms are NOT run against collected FAA 702 data (702 data is contained in MARINA, MAINWAY, NUCLEON, PINWALE (Sweet* and Sour* partitions) and other databases).

FASCIA S//SI//REL TO USA, FVEY) FASCIA II is a tool used as the primary source of metadata used in target development within the SIGINT community. The FASCIA II data warehouse contains PSTN, PCS, Media Over IP (MOIP), High Powered Cordless Phone (HPCP) Call Detail Records, ISAT, and VSAT contact events, It formerly contained Digital Network Intelligence (DNI) contact events which are now in MARINA. Analysts may login to FASCIA II to utilize its query and reporting facilities to identify and locate targets based on these call events, as well as adjust collection. FASCIA II also delivers high volumes of data to multiple data marts and follow-on analytical tools that aid in target development within the Intelligence Community. The number of users that have direct access to the FASCIA II database is restricted. Therefore, most analysts access FASCIA II data through BANYAN, a calling-tree analysis tool which contains all FASCIA II call records and LAMPSHADE INMARSAT data. Other tools that access FASCIA data include ASSOCIATION, MAINWAY, HOMEBASE and SEDB.

FISA Foreign Intelligence Sureveillance Act-governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. A complete copy of the Act is found at Annex B to NSA/CSS Policy 1-23. The Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States, all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy. The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General. (from: USSID SP0018 / Annex A – Procedures for Implementing Foreign Intelligence Surveillance Act)

FRIAR (TS//SI//NF) FAIRVIEW's covername for the east coast cable station

IP Internet Protocol-a protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one address that uniquely identifies it from all other computers on the Internet, with exceptions such as NAT (Network Address Translation) and the use of non-routable private address ranges. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an

adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

KEYCARD (S//SI//REL) KEYCARD is the premier Target-based Filtering and Selection database. KEYCARD is an integral part of the TURMOIL collection system and a member of the TURBULENCE suite of tools. Using smart-collection capabilities, KEYCARD has transformed the way target-based development and collection is performed. KEYCARD rapidly determines whether data should be collected or ignored. Analysts develop targets for selection via the Unified Targeting Tool (IRISHBEAUTY), OCTAVE and the KEYCARD GUI.
KK (TS//SI//NF) KOZYKOVE-A FAIRVIEW site

KOZYKOVE (TS//SI//NF) A FAIRVIEW site

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

LOPERS (S//SI//REL) LOPERS is a Dialed Number Recognition (DNR) system providing filtering, selection, and metadata extraction for intercepted telephony traffic. With the exception of the signal input card, LOPERS is entirely software based and runs on Linux on commodity Intel-based PC hardware. LOPERS also provides the ability to cluster multiple machines to operate as a single DNR system. LOPERS processes telephony traffic found on the Public Switched Telephone Network (PSTN); on GSM, CDMA, and UMTS Core networks; or in between the PSTN and a Core network. Input cards or a network-based Data Distribution Service (DDS) provide intercepted telephony traffic to the LOPERS system. LOPERS decodes the telephone numbers present in the call signaling and forwards the numbers to KEYCARD for normalization and validation. Calls including targeted selectors are captured and saved to an output directory, where MAILORDER picks them up for forwarding to follow-on processing systems. LOPERS offers four flavors of the system: one for use by first- and second-party installations and three different flavors for third-party partners.

LUMBERYARD FAIRVIEW (satisfying POC with NTOC for anomaly detection/ situational awareness)

MAINWAY (TS//SI//REL) MAINWAY, or the MAINWAY Precomputed Contact Chaining Service, is an analytic tool for contact chaining. It's helping analysts do target discovery by enabling them to quickly and easily navigate the increasing volumes of global communications metadata. Mainway attacks the volume problem of analyzing the global communications network. Automated traffic analytic processes support global multi-mode target development, alerting and intelligence reporting. Initial requirements include global contact chaining and timelining of all telephony, e-mail and pager contacts, from both collection and toll records. Automation processes use the global contact chains to identify potential tasking changes, new communities of interest, changes in communities of interest, activity patterns of interest, number normalization

errors, COMSEC changes, and to help score/select content for forwarding and processing. Visualization tools are also available to document findings and help develop new automation algorithms.

MAILORDER U//FOUO) MAILORDER is an FTP-based file transport system used to move data between various collection, processing and selection management systems. Originally developed in 1990, MAILORDER has been ported to many hardware platforms over the years. The current platform runs Linux on Intel x86 hardware with the Sybase ASE 15 database for keeping track of statistics. Ultimately MAILORDER will be replaced by JDTS, but MAILORDER Systems will continue to serve in the Transport Architecture for years to come. MAILORDER relies on information in the filename to determine how to route data. The filename must begin with the PDDG of the originating site. This is followed by a three character File Routing Trigraph, which identifies a destination system and directory. Next is a two character Source System Digraph, which identifies an individual piece of equipment within the given site. Next is a priority digit, a number between one and seven (high to low priority), which is used to prioritize files.

MERLIN (T//SI//NF) FAIRVIEW'S Effort to build-out the mobility network access. It will be a multi-year, multi-phased initiative to exploit various facets of the network, which include SMS messages, Mobile Application Part (MAP), packet data and voice. Consumers are rapidly abandoning traditional telephones and migrating towards mobile devices. Secondly, consumers are also changing the way they communicate, from voice calls to text messages and e-mail. Going forward, it will be essential to have mobile communications as part of the program's comprehensive SIGINT strategy.

NSAH (U//FOUO) National Security Agency Hawaii

NSAW (U//FOUO) National Security Agency Washington

NSOC (U//FOUO) National Security Operations Center

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 imperitive 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.

NUTHATCH (TS//SI//NF) FAIRVIEW'S covername for the transport upgrade between FRIAR/PC access to accommodate growth in the cable system)

OCTAVE (C//SI//REL) OCTAVE is the principal means for tasking of telephone numbers (and other telephone identification data such as IMSIs, IMEIs, and INMARSAT FTINs and RTINs) to the various DNR collection systems used by the National Security Agency and its Second Party partners. It also enables the management of those numbers. Conversely, CONTRAOCTAVE is a reference database that contains phone numbers that should not be tasked in OCTAVE or UTT. OCTAVE is scheduled to be replaced by UTT by 2011. See OCTAVE-UTT-Transition for the approximate timeline.

OPSEC (U//FOUO) Operations Security-the process of denying potential adversaries information about friendly capabilities and intentions by identifying, controlling and protecting generally unclassified indicators associated with planning and conducting operations and other activities.

PBX (U//FOUO) Private Branch Exchange Telephone service provided for a customer's use consisting of central office trunks, a switchboard and extension telephones which may be interconnected with the trunks or with each other through the switchboard and associated equipment. PBXs may be manual or dial, depending on the method used by extensions to place incoming or outgoing calls.

PINECONE (TS//SI//NF) PINECONE-Cover name for the LITHIUM site in NJ for FAIRVIEW

PINWALE (TS//SI//NF) PINWALE is NSA's primary storage, search, and retrieval mechanism for SIGINT text intercept. PINWALE's mission is to provide storage and on-line access to multiple terabytes of DNE and textual data upon analytical requests. It is to provide timely, accurate, and reliable Text Search and Retrieval Support to the user community. Target data is filtered through a Packet Raptor at site before exfill. Once brought back to NSAW, it is processed by a WC2, which is followed by an XKEYSCORE for selection.

PLANK (TS//SI//NF) Access expansion and collection (content and metadata) via the deployment of a global SIGINT sensor grid through FAIRVIEW's LITHIUM partner.

PLANK-3A (TS//SI//NF) The follow-on to FAIRVIEW's FY11 PLANK-3 access expansion effort.

POC (U//FOUO) Point of Contact

POORWILL (TS//SI//NF) FAIRVIEW'S effort to continue cable modernization, specifically focus on providing increased DNR access capacity and processing across all existing cable sites. Additionally, the proposed effort includes increased processing capacity at the Program's centralized processing facility - PINECONE.

PR/TT (TS//SI//NF) Pen Register / Track and Trace collection-terms relating to the collection of metadata under FISA authorities. The definitions of the Pen Register and Trap and Trace techniques were significantly expanded in the USA Patriot Act of 2001. Previously, a pen register only referred to a device that provided a list of all the numbers dialed from or to a particular phone. The Patriot Act expanded the definition of a pen register from just the attachment of a device to a telephone line to include any process that will capture dialing, routing, addressing, or signaling information. A trap and trace device is similar to a pen register, except that the device only captures incoming information. It too was expanded to include dialing, routing, addressing, or signaling. In effect, the definitions were broadened to allow the collection of both telephony and Internet metadata. (Source: PRTT Need to Know Guide dated April 2008).

RAS (TS//SI//NF) Reasonable Articulable Suspicion

RODEO STAR (TS//SI//NF) FAIRVIEW Site

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 imperitive 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.

SERENADE (TS//SI//NF) BLARNEY's covername for one of their Corporate Partner's. Need WPG ECI for name

SG (U//FOUO) STARGATE-FAIRVIEW A site

SC (U//FOUO) SILVERCOLLAM-FAIRVIEW site

SCIF (U//FOUO) Sensitive Compartmented Information Facility

SEALION (TS//SI//NF) A FAIRVIEW site

Selector U//FOUO) A Selector is an identifier used in dialed number recognition (such a telephone number, IMEI, IMSI, or MSISDN) or used in digital network intelligence (such as an email address or instant messaging IDs). A selector becomes a seed once it is RAS approved.

SEAGULL (TS//SI//NF) BR-FISA Metadata, LITHIUM’s billing records

SERENADE (TS//SI//NF) BLARNEY's covername for one of their Corporate Partner's. Need WPG ECI for name

SILVERCOLLAM (TS//SI//NF) A FAIRVIEW site

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.

STARGATE (TS//SI//NF) A FAIRVIEW site

STONEGATE (S//SI//REL) STONEGATE is an automated and scalable dial-up data modem and FAX modem demodulation system. It is used to collect, recognize, demodulate, format, forward, database, archive, and reporting on dial-up data modem, FAX modem, speech, and unknown signals. STONEGATE is designed to handle the 80% of the dial-up data modem and FAX modem traffic that can be automatically and correctly processed. The 20% of the traffic that can not be automatically and correctly processed is forwarded to a demodulation system that has the resources needed to process the traffic. If there are problems with the STONEGATE processed signal, the original signal can be automatically retrieved via the Archive Retrieval interface. Speech and unknown traffic are detected and forwarded. STONEGATE generates statistics and

reports on dial-up data modem, FAX modem, speech, and unknown signals.

TITANPOINTE (TS//SI//NF) BLARNEY'S site in NYC

TU (U//FOUO) TURBULENCE

TUBE (C//SI//REL) TUBE is the TU Back-end; it receives SOTF objects from TML (and potentially other TU systems), determine what forwarding actions should occur, and perform any requisite pre-forwarding preparation processing so as to create objects which can be ingested by the appropriate destination repositories. This includes 2nd and 3rd party legacy databases. TUBE will also forward objects to PWV in SOTF format.

TURBULENCE (TS//SI//REL) TURBULENCE is the Enterprise framework of mission modernization, an element of the Enterprise Architecture. As part of NSA/CSS Transformation, TURBULENCE unifies MidPoint and Endpoint SIGINT, and dynamic defense, and enables network attack in a manner that creates cooperative, interoperable, real-time exploitation/defense/attack-enabling capabilities between geographically distributed nodes in a peer-to-peer (P2P) manner. At one time TURBULENCE was equivalent to NCC, or more precisely, the NCC acquisition program was tasked to acquire TURBULENCE. However, in CY2008 acquisition responsibility for some parts of the TURBULENCE architecture were split off to other program offices so that the NCC program is now responsible for some but not all components of TURBULENCE.

TURMOIL (S//SI//REL) TURMOIL is the passive Digital Network Intelligence (DNI) SIGINT collection component of the TURBULENCE architecture, funded by the Network Centric Capabilities (NCC) acquisition program. It consists of an architecture designed to be extensible and flexible, so that the collection posture on these accesses can be altered dynamically with minimal service interruption. TURMOIL delivers IP data, sessionized and processed, to the back-end of the SIGINT system, in an analyst-ready form.

VPCS (U//FOUO) Virtual Passive Collection Suite-a collection of virtualized components of the TURBULENCE collection system targeted for lower speed environments. The Virtual Machine (VM) images provide a fully functional passive collector suite, development environment, and testing environment in one system.

XKEYSCORE (S//SI/REL) XKEYSCORE is a computer network exploitation system that combines high-speed filtering with SIGDEV. XKEYSCORE performs filtering and selection to enable analysts to quickly find information they need based on what they already know, but it also performs SIGDEV functions such as target development to allow analysts to discover new sources of information. XKEYSCORE processes data at field sites, where it is collected, and allows analysts from all over the world to query it. At field sites, the XKEYSCORE software can run in clusters of few or many computers, giving it the ability to scale in both processing power and storage. All processing is plug-in based, which allows new capabilities to be quickly deployed to support operational

needs. XKEYSCORE, in various configurations, is deployed around the world and is used by each FVEY partner.

XKS (U//FOUO) XKEYSCORE