NATIONAL SECURITY AGENCY/CENTRAL SERCURITY SERVICE

EXCEPTIONALLY CONTROLLED INFORMATION (ECI)

AS OF 12 SEPTEMBER 2003

(S) This document contains a total listing of National Security Agency/Central Security Service Exceptionally Controlled Information (ECI). Dissemination and extraction of information from this document is controlled by the originator.

(S) This listing is highly sensitive and must be strictly controlled on a need-to-know basis and only used for specific ECI management or other administrative needs as approved by the Director, NSA (DIRNSA).

(S) This list is not to be reproduced by physical or electronic means unless expressly authorized by DIRNSA or his designated representative.

(U)ECI Coverterm	(U)Trigraph	(U) Protected Information	(U) Overlapping Programs
(U//FOUO) ABEYANT	(U) N/A	(TS//SI) Protects information related to sensitive SIGINT Enabling relationships.	(S) Encompasses four ECIs: APERIODIC, AUNTIE, AMBULANT, and FIRSTDOWN
(U//FOUO) AMBULANT	(U//FOUO) AMB	(TS//SI) Protects information related to sensitive SIGINT Enabling relationships.	(S) Under ABEYANT program
(U//FOUO) APERIODIC	(U//FOUO) APR	(TS//SI) Protects information related to sensitive SIGINT Enabling relationships.	(S) Under ABEYANT program
(U//FOUO) AUNTIE	(U//FOUO) APR	(TS//SI) Protects information related to sensitive SIGINT Enabling relationships.	(S) Under ABEYANT program
(U//FOUO) BOATMEN	(U//FOUO) BTM	(TS//SI//NF) Feasibility study for special exfiltration initiatives between NSA and a Third Party.	(U) N/A
(U//FOUO) BOXWOOD	(U//FOUO) BXD	(TS//SI//NF) Protects a sensitive sole source of lucrative communications intelligence emanating from a target.	(U) N/A
(U//FOUO) BULLET	(U//FOUO) BLT	(TS//SI//NF)Protects NSA's potential assistance in reconstituting a Third Party's SIGINT collection capability.	(U) N/A
(U//FOUO) CHILLY	(U//FOUO) CHI	(TS//SI//NF) Protects details of NSA association with and active participation in planning and execution of sensitive Integrated Joint Special Technical Operations (IJSTO) offensive Information Warfare (IW) strategies.	(TS//SI//NF) IJSTO is the US Government process for the planning, deployment and employment of Special Access Program (SAP) weapons
(U//FOUO) CLERIC	(U//FOUO) CLC	(TS//SI) Protects policy exchanges between NSA and GCHQ related to Special Source activities.	(U) N/A
(U//FOUO) CONQUERER	(U//FOUO) CON	(TS//SI//NF) Protects fact of joint NSA/CIA clandestine Radio Frequency operations.	(S) CIA's KLAMATH (KLM) Control Channel
(U//FOUO) DECKSTOP	(U//FOUO) DKP	(TS//SI//NF) Protects information that would reveal clandestine SIGINT sources of collection against a high priority target's internal domestic communications.	(U) N/A
(U//FOUO) DICHOTOMY	(U//FOUO) DCH	(TS//SI) Protects raw traffic and signals reporting information gained from especially sensitive (perishable) and clandestine sources.	(U) Disestablished on 1 Oct 03.
(U//FOUO) DILEMMA	(U//FOUO) DLM	(TS//SI) Summary description – A dormant ECI. A failed attempt to convince an IC partner to remove the "Fact Of" a particular collection capability from their tightly controlled channel and placed in this ECI	(TS//SI) Relates to a US Military unacknowledged SAP and Control System referred to at NSA as RAMPART M.
(U//FOUO) DOMINATE	(U//FOUO) DOM	(TS//SI//NF) Protects sensitive sources and methods used to determine the frequencies targeted by a target COMINT collection system.	(C) All intelligence derived under this program is handled via FLEXURE reporting channels.

(U//FOUO) ENSIGN	(U//FOUO) ENS	(TS//SI//NF) Protects potential NSA partnership with a Third Party in clandestine SIGINT activity in a specific location.	(TS//SI//NF) STAIRWELL also covers NSA partnership with this Third Party in unconventional SIGINT initiatives.
(U//FOUO) ESCAPEE	(U//FOUO) ESCP	(TS//SI//NF) U.S. component to ECI STATEROOM	(U//FOUO) STATEROOM
(U//FOUO) EVADEYIELD	(U//FOUO) EVY	(TS//SI//NF) Protects NSA's capability to exploit voice or telephonic conversations from an extremely sensitive source.	(U) N/A
(U//FOUO) FIRSTDOWN	(U//FOUO) FRS	(TS//SI) Protects information related to sensitive SIGINT Enabling relationships.	(S) Under ABEYANT program
(U//FOUO) FLEXURE	(U//FOUO) FLX	(S) Protects military and civilian assets from detection by an adversary.	(S) Works with data collected by DOMINATE
(U//FOUO) FORBIDDEN	(U//FOUO) FBD	(TS//SI//NF) Protects information pertaining to joint operations conducted by NSA, GCHQ, CSE, CIA, and FBI against foreign intelligence agents.	(U) N/A
(U//FOUO) FORBORNE	(U//FOUO) FBR	(C//REL TO USA, CAN, AND GBR) Protects the fact that the National Security Agency, GCHQ, and CSE can exploit ciphers used by hostile intelligence services.	(U) N/A
(U//FOUO) GRAYSCALE	(U//FOUO) GRL	(TS//SI//REL TO USA, AUS, CAN, GBR AND NZL) Protects information that could allow Second-Party-partner-assisted network infiltration operations to be detected and recognized.	(U) N/A
(U//FOUO) HELLFIRE	(U//FOUO) HLF	(TS//SI//NF) Protects activities of non-INFOSEC elements of NSA providing INFOSEC assistance to another non-hostile government.	(U) N/A
(U//FOUO) HISTORY	(U//FOUO) HST	(TS//SI//NF) Protects NSA and certain commercial cryptologic equipment manufacturer relationships.	(U) N/A
(U//FOUO) INVEIGH	(U//FOUO) INV	(S//SI) Protects vendor access to various diplomatic targets within the United States.	(U) N/A
(U//FOUO) INVENT	(U//FOUO) IVT	(TS//SI//NF) Protects NSA partnership with a Third Party in special SIGINT collection efforts in a specific location.	(TS//SI//NF) ENSIGN covers clandestine SIGINT activity with this Third Party as INVENT. STAIRWELL covers unconventional SIGINT activity with this Third Party.
(U//FOUO) LYSERGIC	(U//FOUO) LSG	(TS//SI) Protects NSA's efforts to select and prosecute foreign deployed telecommunications cables as SIGINT targets.	(S) CIA's KLAMATH (KLM) Control System.
(U//FOUO) MISCHIEF	(U//FOUO) MSF	(TS//SI) The highest level of access protecting sources, targets, sites, and unique collection techniques of the BLARNEY program.	(U//FOUO) RAGTIME

(U//FOUO) OPALESCE	(U//FOUO) OPS	(S//SI//REL TO USA, AUS, CAN, GBR AND NZL) Protects Close Access SIGINT collection operations, which require a specialized sensor, positioned in close physical proximity to the target device or facility.	(U) N/A
(U//FOUO) PAWLEYS	(U//FOUO) PAW	(TS//SI) Protects and covers clandestine access to cryptographic information and material. It protects the operational details, as well as any materials, technical information and SIGINT capabilities	(S) CIA is the primary partner organization, which includes the FBI and DIA/DHS through TAREX. Also includes 2nd Party counterpart organizations.
(U//FOUO) PENDLETON	(U//FOUO) PEN	(TS//SI//REL TO USA, AUS, CAN, GBR, NZL) Protects NSA's investment in manpower and resources to acquire our current bottom line capabilities to exploit SIGINT targets by attacking public key cryptography as well as investment in technology.	(U) N/A
(U//FOUO) PIEDMONT	(U//FOUO) PIE	(TS//SI//REL TO USA, AUS, CAN, GBR, NZL) Provides protection to NSA's bottom line capabilities to exploit SIGINT targets by attacking the hard mathematical problems underlying public key cryptography as well as any future technologies as may be developed.	(U) N/A
(U//FOUO) PITCHFORD	(U//FOUO) PIT	(TS//SI) Details of certain cryptographies in which materials have been derived from a sensitive source or method.	(U) N/A
(U//FOUO) RAGTIME	(U//FOUO) RGT	(TS//SI) The second level of access protecting the identity of targets/target locations and cooperative relationships within the BLARNEY program. See MISCHIEF entry.	(U) N/A
(U//FOUO) REFRACTOR	(U//FOUO) RFR	(TS//SI//NF) Protects engineering and operational processes associated with tailoring U.S. Information Assurance equipment for release to and use by foreign countries.	(U) N/A
(U//FOUO) RUBIOUS	(U//FOUO) RBI	(TS//SI//NF) Protects information that could allow otherwise unilateral U.S. network infiltration operations to be detected and recognized.	(U) N/A
(U//FOUO) STAIRWELL	(U//FOUO) STRW	(TS//SI//NF) Protects NSA partnership with a Third Party in unconventional SIGINT activity.	(U//FOUO) ENSIGN and INVENT
(U//FOUO) STATEROOM	(U//FOUO) STRM	(S//SI) Restricts access to information about personnel involved in covert collection, processing and reporting of SIGINT from diplomatic missions abroad. This activity is conducted by USA, AUS, CAN, GBR, and NZL.	(S) U.S.-only version is ESCAPEE

(U//FOUO) STEREO	(U//FOUO) SRO	(TS//SI) The same level of access as ECI RAGTIME, though used to identify those individuals who require special handling/data sanitization training.	(U) N/A
(U//FOUO) STRESSFUL	(U//FOUO) SRF	(TS//SI//NF) Protects exploitation of specific communications associated with individuals and organizations involved in money laundering in support of narcotics traffickers and organized crime targets of interest.	(U) N/A
(U//FOUO) TAXONOMY	(U//FOUO) TXM	(TS//SI) Protects policy exchanges between NSA and CSE related to Special Source activities.	(U) N/A
(U//FOUO) VISITOR	(U//FOUO) VSR	(TS//SI) The lowest level of access protecting the fact of the BLARNEY program and that it is governed by the Foreign Intelligence Surveillance Act.	(U) N/A
(U//FOUO) WASHBURN	(U//FOUO) WSB	(TS//SI) Covers CLANSIG effort with CIA to exploit a SIGINT source in a Middle Eastern location then in the research and analysis phase. ECI created for use solely with GCHQ to shield GCHQ from CIA's NOFORN Control Channel.	(S) CIA's KLAMATH (KLM) Control System.