

TOP SECRET//SI//TK//NOFORN

**NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE**

**(U) CLASSIFICATION GUIDE FOR
SIGINT Material Dating from 16 August 1945 - 31 December 1967**

Effective Date: 21 December 2011

**Revised Date(s): 24 February 2012, 13 April 2012
25 April 2012**

CLASSIFIED BY: [REDACTED]
Intelligence Director

REASON FOR CLASSIFICATION:
1.4(c), 1.4 (d)

**DECLASSIFY ON: *75 years from date of
material or event, as indicated**

ENDORSED BY: [REDACTED]
**Deputy Associate Director for Policy and
Records**

TOP SECRET//SI//TK//NOFORN

TOP SECRET//SI//TK//NOFORN

TOP SECRET//SI//TK//NOFORN

(U) Classification Guide for SIGINT Material Dating Prior to 1 January 1968

(U) PUBLICATION DATE:

(U) OFFICE OF ORIGIN: SID

(U//FOUO) POC: [REDACTED] S02

(U) PHONE: [REDACTED]

(U) ORIGINAL CLASSIFICATION AUTHORITY:
SIGINT Director, [REDACTED]

(U) This classification guide describes the SIGINT material that is dated from 16 August 1945 – 31 December 1967 and warrants protection for more than 50 years. It supersedes all prior guidance relating to material originating during this timeframe. This guidance pertains to NSA/CSS as well as to its predecessor organizations.

Description of Information	Classification/Markings	Reason	Declass	Remarks
<p>1. (U) All sources- and methods- related metadata added to SIGINT product reports by NSA/CSS or included in NSA/CSS metrics reports</p>	<p>CONFIDENTIAL//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(U//FOUO) This includes information such as SIGINT addresses (SIGADs), Producer Designator Digraphs (PDDGs), Case Notations (CASNs), <i>RASIN</i> Manual designators, intercept designators, SRIs, Crypt System Titles, Intelligence Source Indicators (ISIs), Time of Intercept (TOI), Communications Lanes (foreign FROM/TO entities), Message Telex numbers assigned by foreign target, number of messages collected for a specific target, number of messages decrypted for a specific target, etc.</p> <p>(U) Exceptions: For the period of the Vietnam conflict (through 31 December 1967) – all metadata for otherwise releasable reports in which the targeted entity was a participant in the Vietnam conflict is UNCLASSIFIED.</p> <p>(U//FOUO) The methodologies used by</p>

				<p>NSA/CSS to log, track, account for, and analyze collection prior to 1968 are still used today. Revealing this “who,” “when,” “where,” and “how” could provide an adversary with a great deal of insight into NSA’s targets, collection sites, and other collection- and analysis-related information that is still being used today.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>2. (S//NF) Information revealing the fact of NSA/CSS targeting, collecting, or processing the communications of these specific foreign countries/international organizations:</p> <ul style="list-style-type: none"> - Algeria after 31 Dec 1946 - Belgium after 31 Dec 1946 - France after 31 Dec 1946 - Germany (i.e., West Germany) after 31 Dec 1946 - Netherlands after 31 Dec 1946 - Norway after 31 Dec 1946 - Saudi Arabia after 31 Dec 1946 - Sweden after 31 Dec 1946 - Tunisia after 31 Dec 1946 - Turkey after 31 Dec 1946 - Taiwan (Formosa) after 31 Dec 1949 - Italy after 31 Dec 1947 - Jordan after 31 Dec 1947 - Denmark after 31 Dec 1953 - South Korea after 31 Dec 1953 - Japan after 31 Dec 1954 - Austria after 31 Dec 1955 - Israel for any timeframe (see 	<p>SECRET//REL TO USA, FVEY at a minimum</p>	<p>75X1 75X3 75X6</p>	<p>*75 years from either the date of material or the end of the particular partnership, whichever is longer</p>	<p>(U) The fact of NSA/CSS targeting, collecting, or processing against any nation not listed as classified <u>through 1967</u> is UNCLASSIFIED.</p> <p>(U) Revealing these specific targets will enable adversaries to deduce the strength and range of NSA/CSS’s capabilities at that time. When there is direct link between the communications systems used then and those used today, the targets can adopt blanket denial practices not currently used because they simply do not appreciate how well their signals are currently being exploited by NSA/CSS. In addition, certain historical targets are also (and were in the timeframe covered by this guide) SIGINT partners, and revealing that NSA/CSS targeted nations that are current partners could have an immediate negative effect on those relationships.</p> <p>(U) The fact that NSA/CSS processed intercepted Israeli communications during the USS Liberty incident (24</p>

<p>remark for specific exception) - Pakistan for any timeframe - Singapore for any timeframe - all international organizations</p>				<p>May – 8 June 1967) is UNCLASSIFIED.</p> <p>(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>3. (S//NF) Information revealing the fact of NSA/CSS targeting, collecting, or processing the communications of a Second Party country</p>	<p>SECRET//NOFORN</p>	<p>75X1 75X3 75X6 75X9</p>	<p>*75 years from either the date of material or the end of the partnership, whichever is longer</p>	<p>(S//NF) Second Party partnerships are among NSA/CSS's strongest, oldest, and most important. Revealing the fact that NSA/CSS targeted their communications at any time would most likely have serious implications for, and could cause irreparable damage to, the partnerships.</p> <p>(U) Serious damage to national security can be expected if this material were to be declassified.</p>
<p>4. (U) The identities of specific NSA/CSS Third Party SIGINT partners</p>	<p>SECRET//REL TO USA, FVEY at a minimum</p>	<p>75X1 75X3 75X6</p>	<p>*75 years from either the date of material or the end of the particular partnership, whichever is longer</p>	<p>(U//FOUO) NSA/CSS's Third Party partners provide NSA with unique and valuable insights on counterterrorism, combating proliferation, and regional stability issues. They also often provide NSA/CSS information about each other. Although they may suspect they were targets prior to 1968, their level of cooperation with NSA is expected to diminish if it became a known fact. Conversely, if information that NSA/CSS has relating to these countries that is outside the scope of the partnerships were to be released, the countries could gain insight into NSA's other SIGINT capabilities, and could also become aware of information that NSA/CSS has not been sharing. The future of NSA/CSS's Third Party SIGINT foreign partnerships would be at stake.</p>

				(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
5. (U) The fact that NSA/CSS shared particular SIGINT material with a specific Second Party partner, when the partner is identifiable	CONFIDENTIAL//REL TO USA, FVEY at a minimum	75X1 75X3 75X6 75X9	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U//FOUO) NSA/CSS's Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner's work ends and another's starts. In many cases, for a variety of reasons originating within the respective partner's government, Second Party partners insist that their involvement in specific projects or operations must not be released. The UKUSA agreement, signed in 1946, mandates that the Second Parties respect each others' preferences in these cases. (U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
6. (U) The fact that NSA/CSS shared particular SIGINT material with a specific Third Party partner, when the partner is identifiable	SECRET//REL TO USA, FVEY at a minimum	75X1 75X3 75X6	*75 years from either the date of material or the end of the particular partnership, whichever is longer	(U//FOUO) NSA/CSS's Third Party partners provide NSA with unique and valuable insights on counterterrorism, combating proliferation, and regional stability issues. If it were revealed that NSA/CSS shared particular information with specific Third Party partners (essentially revealing the countries with which it had Third Party SIGINT partnerships prior to 1968), the future of its Third Party SIGINT foreign partnerships would be at stake. (U) Serious or exceptionally grave damage to national security can be expected if

TOP SECRET//SI//TK//NOFORN

				this material were to be declassified, depending on the particular information being revealed.
7. (U) Information revealing NSA/CSS targeting, collecting, or processing diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or individual (post 31 December 1946)	SECRET//REL TO USA, FVEY at a minimum	50X1 50X3 50X7	*75 years from date of material	<p>(U) Exceptions:</p> <ul style="list-style-type: none"> - (U) diplomatic/leadership communications collected <i>during and related to</i> the Cuban Missile Crisis (1 January 1959-31 December 1963) are UNCLASSIFIED - (U) North Vietnamese, Laotian, or Cambodian diplomatic/leadership communications related to the Vietnam conflict and collected between 1 January 1960 and 31 December 1975 are UNCLASSIFIED <p>(U//FOUO) Indicating whose diplomatic/leadership communications NSA/CSS targeted, collected, and/or processed prior to 1968 would cause diplomatic challenges for the U.S., and could also enable a targeted country that is still using similar communications systems to change their systems, thereby denying NSA/CSS valuable intelligence.</p> <p>(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
8. (U//FOUO) Information revealing NSA/CSS targeting, collecting, or processing of specific international commercial (ILC) communications (post 31 December 1946)	SECRET//REL TO USA, FVEY at a minimum	50X1 50X3	*75 years from date of material	<p>(U//FOUO) Indicating whose ILC communications NSA/CSS targeted, collected, and/or processed prior to 1968 could also enable a target that is still using similar communications systems to change its systems, thereby denying NSA/CSS valuable intelligence.</p>

TOP SECRET//SI//TK//NOFORN

				(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
9. (U) Information that contains or reveals foreign SIGINT partner equities	CONFIDENTIAL//REL TO USA, FVEY at a minimum	75X1 75X3 75X6 75X9	*75 years from either the date of material or the end of the particular partnership, whichever is longer	<p>(U//FOUO) This includes the basic "fact of" specific Third Party partnerships, names of personnel associated with partner organizations (Second or Third Party), indications of projects that were worked with specific foreign partners (Second or Third Party), collection locations in partner nations (Second or Third Party), etc.</p> <p>(U//FOUO) NSA/CSS's foreign partners provide NSA with unique and valuable insights on a wide variety of issues that are critical to U.S. national security (e.g., counterterrorism, combating proliferation, and regional stability). It is a given that they need to protect their equities as vehemently as NSA/CSS protects its own. If NSA/CSS were to release information that revealed the equities of its foreign partners (Second as well as Third Parties), the future of its SIGINT foreign partnerships would be at stake.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
10. (U//FOUO) Information revealing specific overseas collection and High-Frequency Direction Finding (HFDF) locations that remain open today	CONFIDENTIAL//REL TO USA, FVEY at a minimum	75X1 75X3 75X6	*75 years from either the date of material or closure of site, whichever is longer	(U//FOUO) Revealing specific overseas collection and HFDF locations could adversely affect Third Party SIGINT partnerships and reveal NSA/CSS's HFDF capability strengths and weaknesses. Such revelations

				<p>would identify NSA/CSS's Third Party partners and enable its adversaries to develop countermeasures against its strengths and exploit its weaknesses.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>11. (S//SI//REL TO USA, FVEY) The fact that NSA/CSS conducted/conducts covert SIGINT operations at unspecified officially flagged U.S. facilities abroad</p>	<p>SECRET//SI//REL TO USA, FVEY</p>	<p>75X1 75X3 75X6 75X7</p>	<p>*75 years from either the date of material or end of overall activity, whichever is longer</p>	<p>(S//SI//REL TO USA, FVEY) Revealing the fact that NSA/CSS conducted covert SIGINT operations from officially flagged U.S. facilities abroad would impair the effectiveness of intelligence methods currently in use; would reveal information that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States; and could impair the ability to provide protection services to those U.S. Government officials authorized protection (e.g., President, Vice President).</p>
<p>12. (S//REL TO USA, FVEY) The association of a specific location with an SCS site, the existence of which is releasable to Second Party partners</p>	<p>TOP SECRET//SI//REL TO USA, FVEY</p>	<p>75X1 75X3 75X6 75X7</p>	<p>*75 years from either the date of material or end of overall activity, whichever is longer</p>	<p>(S//SI//REL TO USA, FVEY) Revealing that NSA/CSS conducted covert SIGINT operations from specific officially flagged U.S. facilities abroad would impair the effectiveness of intelligence methods currently in use; would reveal information that would cause serious harm to relations between the U.S. and a foreign government, or to ongoing diplomatic activities of the U.S.; and could impair the ability to provide protection services to those U.S. Government officials authorized protection (e.g., President, Vice President).</p>

TOP SECRET//SI//TK//NOFORN

				(U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
13. (S//REL TO USA, FVEY) The association of a specific location with an SCS site that is NOFORN	TOP SECRET//SI//NOFORN	75X1 75X3 75X6 75X7	*75 years from either the date of material or end of overall activity, whichever is longer	(S//SI//REL TO USA, FVEY) Revealing that NSA/CSS conducted covert SIGINT operations from specific officially flagged U.S. facilities abroad would immediately impair the effectiveness of intelligence methods currently in use; would reveal information that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States; and could impair the ability to provide protection services to those U.S. Government officials authorized protection (e.g., President, Vice President). (U) Exceptionally grave damage to national security can be expected if this material were to be declassified.
14. (U) Information revealing specific sources and methods used by NSA/CSS to target, collect, and/or process SIGINT and that are currently used today	CONFIDENTIAL//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	(U//FOUO) NSA/CSS uses the same sources and methods to obtain SIGINT today as it did prior to 1968. Revealing the specific sources and methods used by NSA/CSS to target, collect, and/or process SIGINT would enable targets to adopt blanket denial practices not used today because they simply do not appreciate how well their signals are currently being exploited by NSA/CSS. (U) See Entry 31 for additional information.
15. (TS//SI//REL TO USA, FVEY) Information revealing the fact of, as well as details relating to, NSA/CSS conducting covert	TOP SECRET//SI//NOFORN	50X1 50X3 50X6	*75 years from date of material	(TS//SI//REL TO USA, FVEY) NSA/CSS's covert SIGINT activities, such as SIGINT enabling and the use

TOP SECRET//SI//TK//NOFORN

<p>SIGINT activities, including material dealing with SIGINT enabling; cover plans, programs, and mechanisms; and/or clandestine SIGINT</p>				<p>of particular cover mechanisms, are much the same today as they were prior to 1968. Revealing the specific covert activities would nullify the particular programs where they are successfully used today. Targets would adopt blanket denial practices not used today because they simply do not appreciate how NSA/CSS's covert activities support SIGINT successes.</p> <p>(U) Exceptionally grave damage to national security can be expected if this material were to be declassified.</p>
<p>16. (U) <i>TICOM</i> documents dated prior to 31 December 1967 where the acquired document was originally created by the U.S. or a Second Party partner and was in the possession of an "enemy" organization.</p>	<p>CONFIDENTIAL//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6 50X9</p>	<p>*75 years from date of material</p>	<p>(U) <i>TICOM</i> documents should only be released if they would have been released by the U.S. or Second Party directly.</p> <p>(U) <i>TICOM</i> documents that may be declassified and released include acquired code books and the description of applications of techniques to cryptographic systems.</p> <p>(U//FOUO) <i>TICOM</i> was a joint Five Eyes effort. NSA/CSS's Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner's work ends and another's starts. In many cases, for a variety of reasons originating within the respective partner's government, Second Party partners insist that their involvement in specific projects or operations must not be released. The UKUSA agreement mandates that the Second Parties respect each others' preferences in these cases.</p>

TOP SECRET//SI//TK//NOFORN

				(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.
17. (U) <i>TICOM</i> interrogation reports	CONFIDENTIAL//REL TO USA, FVEY, at a minimum	50X1 50X3 50X6 50X9	*75 years from date of material	<p>(U) <i>TICOM</i> documents should only be released if they would have been released by the U.S. or Second Party directly.</p> <p>(U) In some cases, <i>TICOM</i> interrogation reports remain not releasable due to <i>BRUSA</i> agreements to protect personal information whose release could reasonably be expected to constitute an unwarranted invasion of personal privacy of a living person.</p> <p>(U//FOUO) <i>TICOM</i> was a joint Five Eyes effort. NSA/CSS's Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner's work ends and another's starts. In many cases, for a variety of reasons originating within the respective partner's government, Second Party partners insist that their involvement in specific projects or operations must not be released. The UKUSA agreement mandates that the Second Parties respect each others' preferences in these cases.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
18. (U) ELINT material related to radar/weapons systems that are still used today	S//REL TO USA, FVEY at a minimum	50X1 50X3	*75 years from date of material	(U//FOUO) Many of the collection and exploitation methods used prior to 1968 continue to be employed in the Intelligence Community.

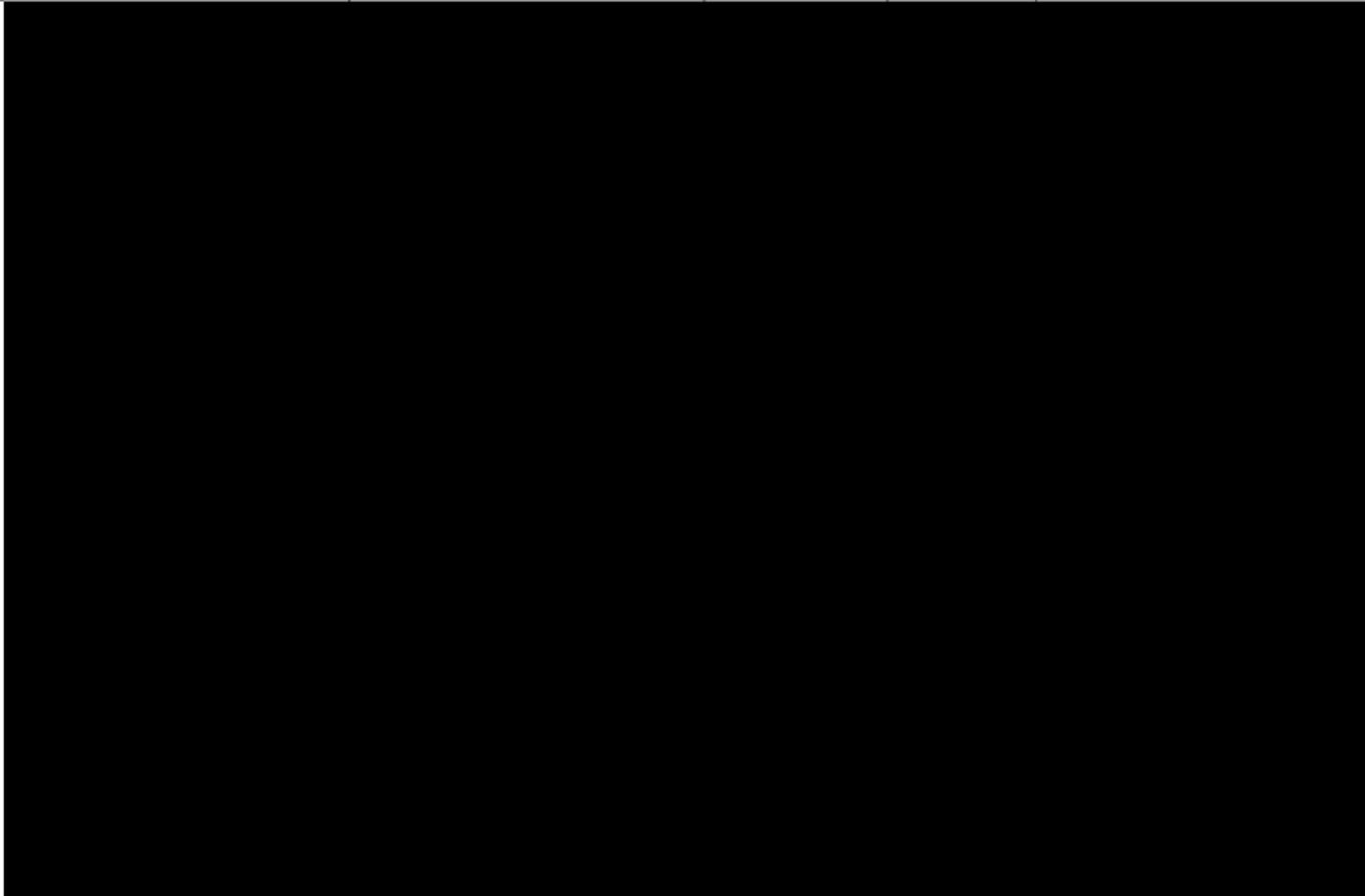
				<p>Declassifying ELINT material that is 50 years old (and older) would enable adversaries, who do not appreciate how well their signals are currently being exploited by NSA, to ascertain those collection and analysis techniques and subsequently adopt denial practices that could preclude further intelligence exploitation. Such denial would hamper intelligence of the modification of old systems as well as the newest ones.</p> <p>(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>19. (U//FOUO) A single ELNOT or list of ELNOTs or designators that equate to specific radars, including those from weapons systems, or similar non-communications signal devices weapons system when associated with amplifying data that identifies the emitter radar, weapon system, country of origin, or ELINT signal acquisition method.</p>	<p>CONFIDENTIAL//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3</p>	<p>*75 years from date of material</p>	<p>(U//FOUO) This category includes information equating a specific ELNOT with a specific radar nickname, such as a NATO nickname, or a radar model number.</p> <p>(U//FOUO) A single ELNOT or list of ELNOTs or designators, e.g., B329A, 1222Z, T6090, 123MZ, when used without amplifying data that identifies the emitter radar, weapon system, or country of origin, or ELINT signal acquisition method is UNCLASSIFIED</p> <p>(C//REL TO USA, FVEY) Examples: - the fact that P307Z and P334A emanate from the Crotales surface-to-air missile is classified CONFIDENTIAL//REL TO USA, AUS, CAN, GBR, NZL - the fact that A427B emanates from SLOT BACK radar is</p>

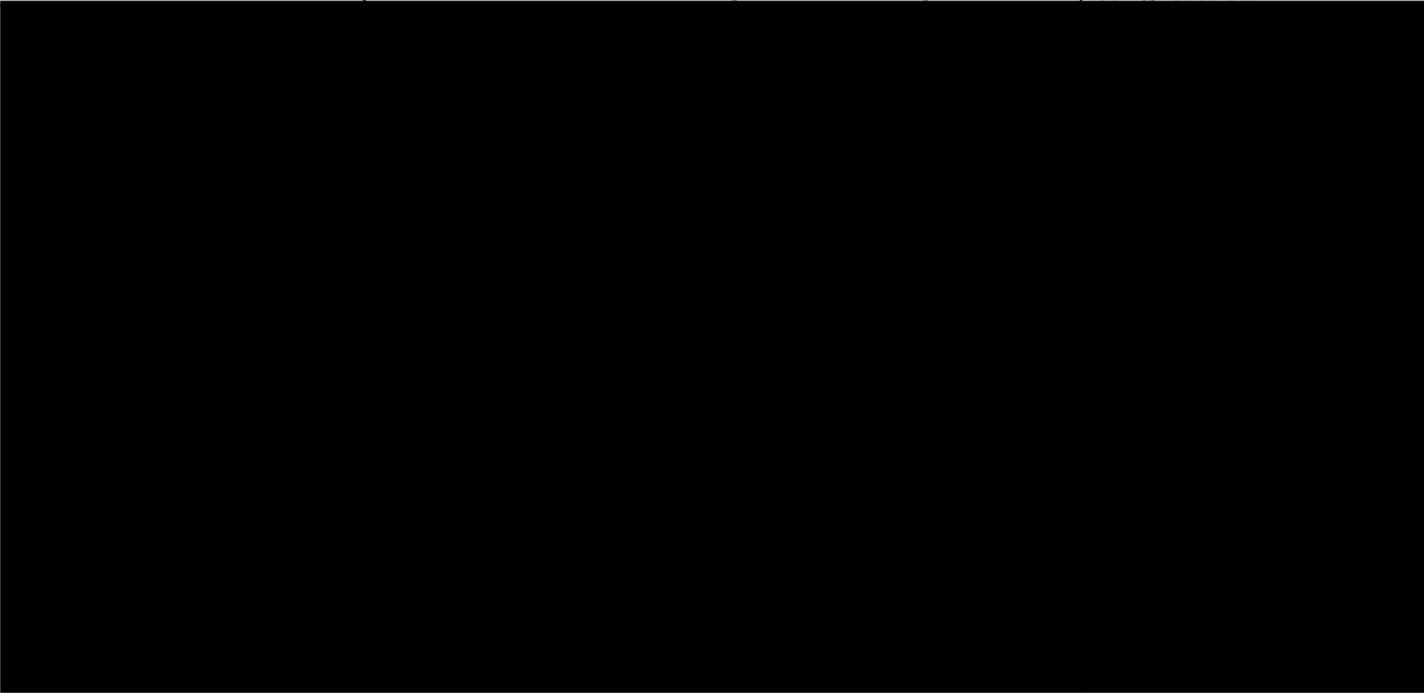
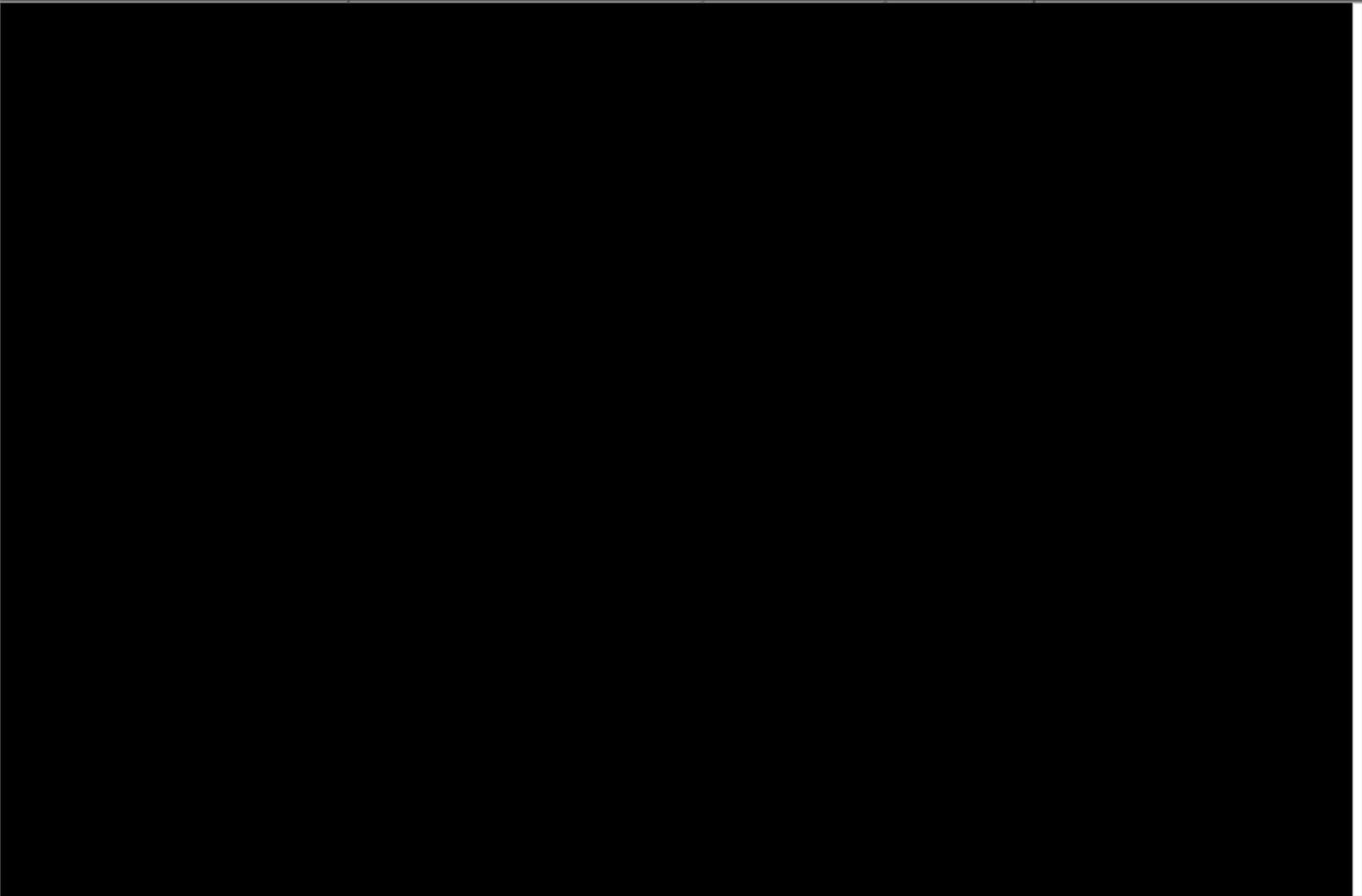
				<p>CONFIDENTIAL//REL TO USA, AUS, CAN, GBR, NZL</p> <p>(U//FOUO) Many of the collection and exploitation methods used prior to 1968 continue to be employed today. Declassifying ELINT material that is 50 years old (and older) would enable adversaries, who do not appreciate how well their signals are currently being exploited by NSA, to ascertain those collection and analysis techniques and subsequently adopt denial practices that could preclude further intelligence exploitation. Such denial would hamper intelligence of the modification of old systems as well as the newest ones.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>20. (U//FOUO) FISINT-related material (i.e., information related to collection, processing, and analysis of telemetry and beacons, command uplinks, video data links, tracking, and arming/fusing/command signals as well as reporting based on said data types)</p>	<p>SECRET//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3</p>	<p>*75 years from date of material</p>	<p>(U) Exceptions:</p> <ul style="list-style-type: none"> - Refer to the following Information Management Instructions (IMIs) for guidance on specific UNCLASSIFIED FISINT-related information: <ul style="list-style-type: none"> - DEFSMAC IM1 ([REDACTED]) - Soviet Deep Space Telemetry Collection IM1 ([REDACTED]) <p>(U//FOUO) FISINT activity began in 1956, and amounts to information that weapons designers use to verify weapon system performance capabilities. The exact</p>

				<p>collection and exploitation methods used from that time are still being used successfully today.</p> <p>(U//FOUO) Declassification of FISINT-related material that is 50 years old and older would show NSA/CSS's ability to fully exploit the data, even with the lack of an identification key and poor signal quality, and likely lead to widespread data denial practices among target countries who do not currently appreciate how well their signals are currently being exploited by NSA. This would deprive the U. S. of vital knowledge of foreign weapons and space systems, which in turn would ultimately lead to policy decisions being made on faulty/incomplete data and to increased loss of life and mission failure during future military operation.</p> <p>(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>21. (U//FOUO) SIGINT material pertaining to counterespionage efforts that reveal NSA/CSS knowledge, exploitation, and analysis of adversaries' tradecraft that is still being used today</p>	<p>TOP SECRET//SI//NOFORN</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(C//REL TO USA, FVEY) Foreign intelligence services' tradecraft is unique to the individual service. Declassifying information indicating that NSA/CSS has successfully exploited their activities, or that it understands their methodologies, would enable the adversaries to refine or alter their practices to the point where it might be denied the information/access entirely (an example would be cover names of agents of an adversary's intelligence service). Adversaries'</p>

				<p>underlying tradecraft (including communications methods and patterns, and all aspects of recruitment and handling of agents) generally remains the same over time, and must be protected in order to maintain NSA/CSS's ability to exploit it. In addition, such material may reveal the identities of a person, or the cooperation of a still-living person, who was the source of information for evidence that was compiled against spies who were later arrested, causing that person's life to be in jeopardy.</p> <p>(U) Exceptionally grave damage to national security can be expected if this material were to be declassified.</p>
--	--	--	--	---

22.



				declassified, depending on the particular information being revealed.
23.				
24.				

<p>25. (U) SIGINT serialized Product Reports that contain <i>cryptologic information</i></p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(C//REL TO USA, FVEY) Releasing decrypts allows the target to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the cryptologies used then and those used today, a straightforward interpolation would allow the target who builds and uses <i>indigenous logics</i> to determine the minimum strength required to defeat NSA/CSS's diagnosis and exploitation today. They can then build and deploy stronger logics or design and deploy logics using different crypto-principles than those used previously. When commercially available logics were used, the target can buy stronger logics or purchase from a different supplier, again with strength and crypto design principles to defeat NSA/CSS's exploitation. When NSA/CSS releases a selected target's decrypts, it has already seen substantive changes in that target's use of cryptography.</p>

				<p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>26. (U) SIGINT serialized Product Reports consisting of or containing decrypts for the <i>Soviet Bloc</i> or People's Republic of China for the period 1 January 1951 through 31 December 1967</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(S//SI//REL TO USA, FVEY) SIGINT serialized product reports for the <i>Soviet Bloc</i> or People's Republic of China consisting of or containing decrypts for the period 16 August 1945 through 31 December 1950 are UNCLASSIFIED, as long as all relevant sources- and methods-related metadata has been redacted.</p> <p>(U//FOUO) Relevant sources- and methods-related metadata includes post-<i>BRUSA system titles</i>, which did not exist until 1946 and comprised a combination of four or more letters and/or numbers. In addition, it includes case notations, <i>RASIN</i> Manual designators, and intercept designators, which are not strictly cryptanalytic, but have relevance to cryptanalytic equities.</p> <p>(U) Information revealing NSA/CSS targeting, collecting, or processing of diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or individual - for any timeframe - remain classified, except for those decrypted using techniques declassified in the versions of <u>Military Cryptanalytics I and II</u>, written by [REDACTED]</p>

				<p>released by NSA, that were collected during and related to the Cuban Missile Crisis (1 January 1959-31 December 1963), and North Vietnamese, Laotian, or Cambodian diplomatic/leadership communications collected prior to 31 December 1975, which are UNCLASSIFIED.</p> <p>(C//REL TO USA, FVEY) Releasing decrypts allows the target to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the cryptologics used then and those used today, a straightforward interpolation would allow the target who builds and uses <i>indigenous logics</i> to determine the minimum strength required to defeat NSA/CSS's diagnosis and exploitation today. They can then build and deploy stronger logics or design and deploy logics using different crypto-principles than those used previously. When commercially available logics were used, the target can buy stronger logics or purchase from a different supplier, again with strength and crypto design principles to defeat NSA/CSS's exploitation.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>27. (U) SIGINT serialized Product Reports consisting of or containing decrypts for North Korea for the period 1 July 1951 through 31 December 1967</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(S//SI//REL TO USA, FVEY) SIGINT serialized product reports for North Korea consisting of or containing decrypts for the period 16 August 1945</p>

			<p>through 30 June 1951 are UNCLASSIFIED, as long as all relevant metadata, including sources- and methods-related information, has been redacted.</p> <p>(U//FOUO) Relevant sources- and methods-related metadata includes post-<i>BRUSA system titles</i>, which did not exist until 1946 and comprise a combination of four or more letters and/or numbers. In addition, it includes case notations, <i>RASIN</i> Manual designators, and intercept designators, which are not strictly cryptanalytic, but have relevance to cryptanalytic equities.</p> <p>(U) All reports by Korea-based field units based on the exploitation of manual codes and ciphers, provided they make no connection to encrypted communications, during and related to the Korean War, 25 June 1950 – 31 December 1953 are UNCLASSIFIED.</p> <p>(U) Information revealing NSA/CSS targeting, collecting, or processing of diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or individual - for any timeframe - remain classified, except for those decrypted using techniques declassified in the versions of <u>Military Cryptanalytics I and II</u>, written by [REDACTED] and officially released by NSA, that were</p>
--	--	--	--

				<p>collected during and related to the Cuban Missile Crisis (1 January 1959-31 December 1963), and North Vietnamese, Laotian, or Cambodian diplomatic/leadership communications collected prior to 31 December 1975, which are UNCLASSIFIED.</p> <p>(C//REL TO USA, FVEY) Releasing decrypts allows the target to deduce the strength and range of NSA/CSS's capabilities at that time. When there is direct link between the cryptologies used then and those used today, a straightforward interpolation would allow the target who builds and uses <i>indigenous logics</i> to determine the minimum strength required to defeat NSA/CSS's diagnosis and exploitation today. They can then build and deploy stronger logics or design and deploy logics using different crypto-principles than those used previously. When commercially available logics were used, the target can buy stronger logics or purchase from a different supplier, again with strength and crypto design principles to defeat NSA/CSS's exploitation.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>28. (U) SIGINT serialized Product Reports consisting of or containing decrypts for any other target (i.e., not <i>Soviet Bloc</i> or People's Republic of China from 1 Jan 1951-31 Dec 1967, not North Korea from 1 July 1951-31 Dec 1967) for the</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(U) Information revealing NSA/CSS targeting, collecting, or processing of diplomatic or leadership communications of a specific foreign country/countries, international organization, group of individuals, or</p>

				<p>target's decrypts, it has already seen substantive changes in that target's use of cryptography.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>29. (U) <i>Alphabet Generators</i>: Documents that demonstrate or include the application of any cryptanalytic technique relating to <i>Alphabet Generator</i> systems that became operational <i>after</i> 15 August 1945</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(U) A document that demonstrates or includes the application of any cryptanalytic technique to an electromechanical cipher system that is an <i>alphabet generator</i> is UNCLASSIFIED only if the system is UNCLASSIFIED in accordance with the WWII Guidance.</p> <p>(U) This guidance pertains to documents relating to:</p> <ul style="list-style-type: none"> • Wired wheels (such as ENIGMA), • Telephone selectors (such as PURPLE, RED, JADE, and CORAL), and Hagelin <i>alphabet generators</i>. <p>(C//REL TO USA, FVEY) In this time frame, commercial companies and nation states developed and deployed cryptographies which have many features still in use in cryptosystems NSA/CSS exploits today. Documents that detail the application of cryptanalytic techniques to these earlier systems will reveal capabilities still in use today against operational target cipher systems.</p> <p>(U) Various levels of harm to national security can be expected if this material were</p>

				to be declassified, depending on the particular information being revealed.
<p>30. (U) Cryptosystems Other Than <i>Alphabet Generators</i>: Documents that demonstrate or include the application of a cryptanalytic technique to any cipher system other than an <i>alphabet generator</i></p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(U) This guidance includes documents relating to any electromechanical systems that are <i>key generators</i>, to include Hagelin <i>key generators</i> and TUNNY.</p> <p>(U) Exception: When a document only contains specific previously declassified techniques applied to a <i>low-grade</i> or <i>medium-grade</i> cryptographic system, the document will be UNCLASSIFIED unless it deals with the application of <i>depth reading</i> or <i>depth-reading</i> techniques. Previously declassified techniques are those declassified in the versions of <u>Military Cryptanalytics I</u> and <u>II</u>, written by [REDACTED] [REDACTED] officially released by NSA.</p> <p>(U) <i>Cryptanalytic worksheets</i> remain classified if they:</p> <ul style="list-style-type: none"> - are for <i>key generators</i>, and/or - indicate <i>depth</i> or <i>depth-reading</i> techniques (e.g., have different cipher texts associated with the same key) - are associated with a specific operational target <p>(C//REL TO USA, FVEY) In this time frame, commercial companies and nation states developed and deployed cryptographies which have many features</p>

				<p>still in use in cryptosystems NSA/CSS exploits today. Documents that detail the application of cryptanalytic techniques to these earlier systems will reveal capabilities still in use today against operational target cipher systems.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>31. (TS//SI//REL TO USA, FVEY) Commercial Cryptanalytic Relationships: Documents that contain information that implies that commercial companies cooperate with NSA/CSS or Second Party partners to render their products exploitable from a cryptanalytic standpoint</p>	<p>TOP SECRET//SI//REL TO USA, FVEY</p>	<p>75X1 75X3 75X6 75X9</p>	<p>*75 years from either the date of material or end of the relationship, whichever is longer</p>	<p>(U) Such documents may also be compartmented.</p> <p>(TS//SI//REL TO USA, FVEY) Exposure of any company's commercial cryptanalytic relationship with NSA/CSS, even for a company no longer in existence, will damage NSA/CSS's credibility with current companies who are approached for assistance. Exposure of even decades-old commercial cryptanalytic relationships may cause significant harm to the company's reputation and financial status.</p> <p>(U) Exceptionally grave damage to national security can be expected if this material were to be declassified.</p>
<p>32. (C//REL TO USA, FVEY) Commercial Information Security Devices: Documents containing details of commercially available cryptographic algorithms, information security devices, or systems that identify an actual vulnerability not currently publicly known, or details relating to NSA/CSS exploitation of a publicly known vulnerability</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(C//REL TO USA, FVEY) Disclosing details of vulnerabilities or NSA/CSS's methods of choice for exploitation will allow commercial companies to fix those weaknesses in existing systems and avoid implementing them in future systems. Frequently, commercial companies make the same or similar mistakes through several generations of their products.</p>

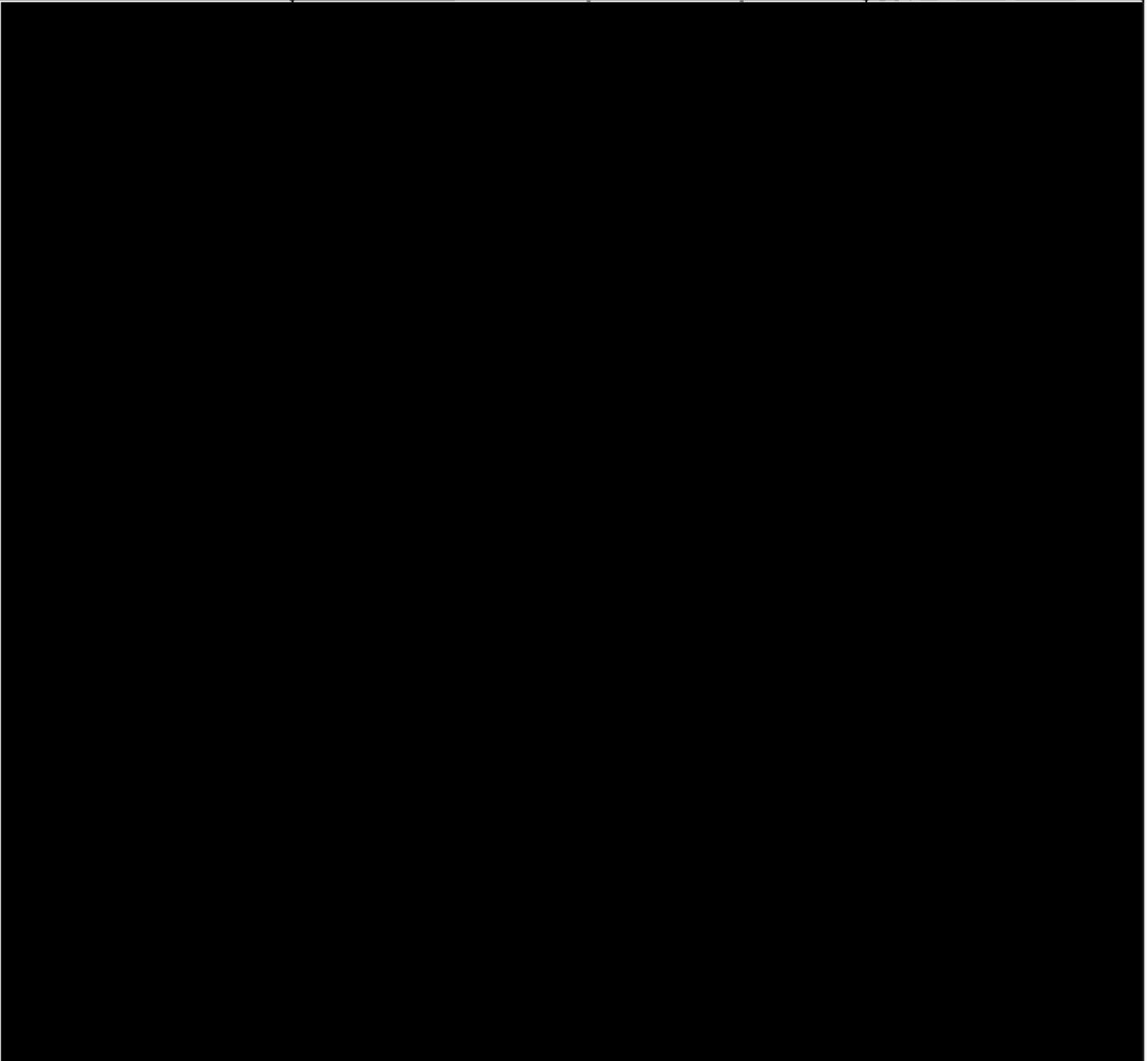
				<p>(U) Information Security Devices provided to other countries by the U.S. Government are considered Commercial Information Security Devices.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>33. (U) <i>Indigenous</i> Information Security Devices: Documents containing details of <i>indigenous</i> cryptographic algorithms, information security devices or systems</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(C//REL TO USA, FVEY) For <i>indigenous</i> security devices or systems, any documents revealing NSA/CSS's knowledge of the cryptography of those devices will risk its ability to diagnose and exploit these devices, and in some cases, knowledge it received from sensitive HUMINT sources.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
<p>34. (U//FOUO) Signal designators when combined with <u>any</u> details that would reveal a target user/country or when associated with cryptanalytically relevant information, such as UKUSA nicknames, coverterms, or any targeting, collection, or exploitation details</p>	<p>CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum</p>	<p>50X1 50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(U//FOUO) Examples of signal designators include <i>RASIN</i> Manual designators and <i>TEXSIGs</i>.</p> <p>(U//FOUO) Signal designators with no indication of target user or country are UNCLASSIFIED.</p> <p>(U) This information is directly linked to NSA/CSS sources and methods for collection and processing. The Second Party standards and notation developed under UKUSA are still in use today.</p> <p>(U) Various levels of harm to national security can be expected if this material were to be declassified, depending</p>

TOP SECRET//SI//TK//NOFORN

				on the particular information being revealed.
35. (U//FOUO) Documents dated after December 31, 1956 that demonstrate or include the application of a signals analytic technique to any digital or digitized system	CONFIDENTIAL//SI//REL TO USA, FVEY at a minimum	50X1 50X3 50X6	*75 years from date of material	
36. (S//REL TO USA, FVEY) Information identifying specific organizations or government agencies that facilitated NSA/CSS <i>close access</i> operations	SECRET// REL TO USA, FVEY	50X1 50X3	*75 years from date of material	<p>(U) These organizations may be U.S. companies, specific units within a U.S. government agency, U.S. national laboratories, or U.S. academic institutions.</p> <p>(S//REL TO USA, FVEY) Revealing the organizations that facilitated <i>close access</i> operations would have a high probability of enabling those to conduct operations in which those organizations continue to have a role or had a role in the past (even if the organization is now defunct).</p> <p>(U) Inclusion damage to national security can be expected if this material were to be declassified.</p>
37. (S//REL TO USA, FVEY) The fact that NSA/CSS has successfully conducted and has an organization devoted to <i>close access</i> operations	SECRET// REL TO USA, FVEY	50X3	*75 years from date of material	<p>(S//REL TO USA, FVEY) The exact collection and exploitation methods used prior to 1968 are still being used successfully today. Declassifying <i>close access</i></p>

				<p>material that is 50 years old (and older) will enable targets to adopt blanket denial practices not used today because they simply do not appreciate how well their signals are currently being exploited by NSA/CSS.</p> <p>(U) Serious damage to national security can be expected if this material were to be declassified.</p>
--	--	--	--	---

38.



				<p>magnetometers, accelerometers, and commercial microphones. This includes information dealing with receivers and the use of radar systems against mechanical or electromechanical office equipment, as well as tools/techniques no longer being used (such as magnetometers, accelerometers, audio signals, power and/or signal line clamps) and that have little chance of future use.</p> <p>(S//REL TO USA, FVEY) Indications that NSA has knowledge of specific and/or unusual parameters, or of NSA's capabilities, could provide information that could be used to understand and counter the collection capability.</p> <p>(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
39. (S//REL TO USA, FVEY) Information describing concealment /camouflage techniques for sensors/systems used in NSA/CSS <i>close access</i> operations	SECRET//SI// REL TO USA, FVEY at a minimum	50X3 50X6	*75 years from date of material	<p>(U) While removal of such sensors/systems is desired once a facility is no longer of interest, is not always feasible. Inadvertent discovery of such systems/sensors could jeopardize future operations and/or raise questions about or point to NSA's involvement.</p> <p>(U) Serious or exceptionally grave damage to national security can be expected if this material were to be declassified, depending on the particular information being revealed.</p>
40. (S//REL TO USA, FVEY) Information that identifies a	TOP SECRET//SI// REL TO USA, FVEY at a minimum	50X3 50X6	*75 years from date	(S//REL TO USA, FVEY) Covert or clandestine

<p>specific target, contains details or parameters relating to specific targets, and/or contains details that could possibly identify a covert or clandestine listening post used by NSA/CSS</p>			<p>of material</p>	<p>Listening Posts (LPs) are physical locations that are close to the target facility and serve as a collection point for the signals of interest. Identification of a LP could result in the identification of information such as the identities of cooperating parties/people. Exposure of such information could adversely impact current and future operations by revealing information about partner relationships.</p> <p>(U) Exceptionally grave damage to national security can be expected if this material were to be declassified.</p>
<p>41. (S//SI//REL TO USA, FVEY) Details, including the "fact of," regarding NSA/CSS collection capability against Short Duration Signals (SDS)</p>	<p>SECRET//SI//REL TO USA, FVEY</p>	<p>50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(S//SI//REL TO USA, FVEY) The methods used to exploit SDS signals and radio fingerprinting are basically the same today as they have been during the period of interest. Specific details regarding how NSA/CSS exploits such signals, as well as the physical locations where it may access them, would provide adversaries information they need to deny them to NSA/CSS. Targets of interest could develop countermeasures that would render NSA/CSS's current capability to collect SDS ineffective.</p> <p>(U) Serious damage to national security can be expected if this material were to be declassified.</p>
<p>42. (U//FOUO) Details regarding NSA/CSS ability to perform radio fingerprinting</p>	<p>SECRET//SI//REL TO USA, FVEY</p>	<p>50X3 50X6</p>	<p>*75 years from date of material</p>	<p>(S//REL TO USA, FVEY) The methods used to perform radio fingerprinting are basically the same today as they have been during the period of interest. Specific details regarding how NSA/CSS exploits such signals, as well as the physical locations where it</p>

				<p>may access them, would provide adversaries information they need to deny them to NSA/CSS.</p> <p>Exception: The fact of, and details regarding, U.S. and South Vietnamese use of radio fingerprinting during the Vietnam Conflict (1 January 1960-31 December 1975), as outlined in the Vietnam is UNCLASSIFIED.</p> <p>(U) Serious damage to national security can be expected if this material were to be declassified.</p>
--	--	--	--	--

<p>45. (S//SI//REL TO USA, FVEY) Information regarding NSA/CSS ability to collect and process International Commercial (ILC), non-Second Party government agencies, non-government organizations, and proprietary communications in the radio frequency spectrum via FORNSAT or Terrestrial means</p>	SECRET//SI//REL	50X3 50X6	*75 years from date of material	<p>(S//SI//REL TO USA, FVEY) Fundamental targets have not changed over time and they continue to use the same basic method of communication. If the fact that NSA targeted these entities is released, the commercial providers, government, non-government, and proprietary entities can implement countermeasures that would degrade NSA/CSS's ability to collect and process these communications.</p> <p>(U) Serious damage to national security can be expected if this material were to be declassified.</p>

***75 years from date of material or event, as indicated:** (U) This indicates that the information is classified for *75 years from date a document is created or until the end of the specified event.

ACRONYMS/DEFINITIONS:

Acoustic – (U) Signals related to the production and transmission of sound. Sound is not restricted to audio range signals

Alphabet Generator - (U) A cipher machine that generates a multiplicity of cipher alphabets from the interaction of two or more components. Compare to *key generator*, below.

BRUSA - (U) The 1946 agreement, now known as UKUSA. In Appendix B (of the 26 February 1946 version) the section on standardization describes the functional system to be used for the nomenclature of foreign cryptographic systems. This common system of nomenclature is now called UKUSA *system titles*.

Close Access - (S//REL TO USA, FVEY) Refers to the targeting, collection, and/or processing of unintentional emanations from information processing equipment, as well as a program to develop special unique sensors and systems to collect unintentional (compromising) *emanations* and/or signals from information processing equipment to exploit TEMPEST vulnerabilities. Keywords that could identify *close access* equities include (but are not limited to)

transducer, radiation, conductance, BOOKLET, magnetic probe, *acoustic* probe, magnetometer, accelerometer, microphone, transmitted over copper wire, *emanations*, and unintentional *emanations*.

Cryptologic Information - (U) Information that describes the target's use of cryptographic techniques and processes or of cryptographic systems, equipment, and software and their functions and capabilities, and all cryptographic material.

Cryptanalytic Worksheets - (U) Any records that show methods of analysis of encrypted and/or enciphered information/data. This includes reports, working aids and papers, instructions, informal technical notes, manuals, technical exchange letters, handbooks, listings, collateral documents, procedure files, evaluation plans, specific documentation or records portraying steps, processes, tables, devices, and/or other means employed in cryptanalysis of target communications.

Depth - (U) Texts are said to be in a *depth* relationship when the texts were produced by encrypting two or more different sequences of plain text with the same sequence of key. Related terms include *depth reading/stripping*, flush depth, near *depth*, offset *depth*, partial *depth*, and slid *depth*.

Depth Reading/Stripping - (U) Recovery of plain text and key from messages in *depth*.

Electromagnetic - (U) Signals that are produced as a result of the use of electrical power

Emanations - (U) Unintentional signals, that, if intercepted and analyzed could disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. These signals may be *acoustic*, *electromagnetic*, or optical in nature

Generic - (U) Describes *emanations* and sensors in broad general categories e.g. magnetic, *acoustic*, power line/signal line conductance, electric field emissions or other naturally occurring phenomena. Sensors are transducers which convert physical or electromechanical signals into an electrical signal which can be collected and analyzed.

Indigenous Algorithm, Device, Logic, or System - (U//FOUO) Non-commercial cryptographic information security system, device or component developed by a SIGINT target for their use. *Indigenous* will include target modifications to commercial products and algorithms. If a target-developed version of a commercially available product is cryptographically indistinguishable from the commercial product, it will be considered commercial.

Key Generator - (U) A cipher machine that generates key from the interaction of two or more components. Compare to *alphabet generator*, above.

Listening Post - (U) Physical locations that are close to the target facility and serves as a collection point for the signals of interest

Low-Grade - (U) Pertaining to a cryptosystem which offers only slight resistance to cryptanalysis; for example:

- (1) Playfair ciphers,
- (2) Single transposition,
- (3) Unenciphered one-part codes

Medium-Grade - (U) Pertaining to a cryptosystem which offers considerable resistance to cryptanalysis; for example:

- (1) Strip ciphers,
- (2) Double transposition,
- (3) Unenciphered two-part codes

RASIN - (U) **Radio Signal Notation (RASIN)** - A notation assigned permanently and jointly by DIRNSA and second Party headquarters to a signal after basic signal characteristics have been verified by NSA/CSS or Second Party signals analysts

Soviet Bloc - (U) Cold War adversaries (Soviet Bloc) up to and including 1950: Albania, Bulgaria, Czechoslovakia (after February 1948), East Germany (though the German Democratic Republic was

only established on October 1949, any prior German activities in the Soviet Zone should be considered as East German and within this definition), Hungary, Poland, Romania, USSR, Yugoslavia

System Title - (U//FOUO) Cryptographic system titles are short identification labels used to create a logical reference mechanism for all cryptographic systems and which identifies the users. Cryptographic system titles are assigned on the basis of cryptography, target country, and entity.

TEXSIG – (U//FOUO) **Technical EXtracts of SIGNALS (TEXSIG)** – A unique designator assigned to a new signal by a SIGINT field element (USSS or Second Party) or to a signal under analysis or cryptanalytic development by the headquarters of NSA/CSS and Second Parties (jointly assigned)

TICOM - (U) **Target Intelligence Committee (TICOM)** - TICOM was formed in London in October 1944 as a joint U.S./UK activity to interrogate captured enemy COMINT personnel and to acquire enemy COMINT records and equipment.