NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-52

Issue Date: 16 November 2012
Revised:

CLASSIFIED NATIONAL SECURITY INFORMATION

PURPOSE AND SCOPE

Pursuant to References a-i, this document establishes policy and responsibilities for *classifying*, *safeguarding*, and *declassifying* NSA/CSS *classified national security information*. This policy does not address *controlled unclassified information* or *information* classified under the Atomic Energy Act of 1954, as amended (Public Law 83-703) (Reference j).

The companion manual to this policy, NSA/CSS Policy Manual 1-52 (Reference k), describes in detail the fundamental procedures critical for protecting and accessing NSA/CSS classified national security information.

This policy applies to all NSA/CSS elements and *affiliates*.

KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS

Endorsed by
Associate Director for Policy

DISTRIBUTION:
DJ1
DJ2
DJ6 (VR)
DJ6 (Archives)

Approved for Release by NSA on 08-29-2013, MDR Case # 74497

This Policy is approved for public release.

This Policy supersedes NSA/CSS Policy 1-52, dated 8 January 2007.
OPI: Information Security Policy, DJ2, 969-2882 (secure) or (443) 654-4596 (public).

POLICY

1. NSA/CSS information that has been determined pursuant to Executive Order 13526 (Reference a) or any predecessor order to require protection against *unauthorized disclosure* shall be classified, marked, safeguarded, and declassified in accordance with the provisions of References a-i.

2. NSA/CSS information shall be originally classified only in accordance with Section 1.1. of Reference a. If there is significant doubt as to whether identifiable or describable damage to national security could accrue by originally classifying specific NSA/CSS information, then it shall not be classified. If there is significant doubt as to the level of damage to national security (i.e., damage [CONFIDENTIAL], serious damage [SECRET], or exceptionally grave damage [TOP SECRET]), then the information shall be originally classified at the lower level. NSA/CSS information shall be *downgraded* as applicable and declassified as soon as it no longer qualifies for *classification* because of a determination that disclosure of the information would no longer damage national security.

3. In accordance with Reference a, the Director, NSA/Chief, CSS (DIRNSA/CHCSS) and other officials within NSA/CSS are specifically identified by position title as having the authority to originally classify information. These individuals are referred to as *Original Classification Authorities (OCAs)*. This authority shall be delegated only to officials who have a demonstrable and continuing need to exercise such authority and shall be limited to the minimum number required for the effective operation of the NSA/CSS. In the absence of an OCA, a person who is appropriately trained and designated in writing to act on the OCA's behalf may exercise this authority. NSA/CSS OCAs also act as the *Declassification Authority* for information under their purview.

4. Failure to comply with this policy may be a violation of the terms imposed by a nondisclosure agreement pertaining to NSA/CSS activities and Federal law and may lead to civil, administrative, and/or criminal sanctions. Such noncompliance shall be immediately reported to the Associate Director for Security and Counterintelligence (ADS&CI) for review and, as appropriate, investigation.

PROCEDURES

5. NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Manual" (Reference k and successor versions) describes in detail the procedures for classifying, safeguarding, and declassifying NSA/CSS classified national security information pursuant to Executive Order 13526, "Classified National Security Information" (Reference a); Intelligence Community Directive (ICD) 700, "Protection of National Intelligence" (Reference d); ICD 710, "Classification and Control Markings System" (Reference e); Department of Defense Manual (DoDM) 5200.01, Vols. 1-3 (References f-h); Executive Order 12333, "United States Intelligence Activities," as amended (Reference l); and DoD Directive 5100.20, "The National

Security Agency and Central Security Service‖ (Reference m). Additional Intelligence Community (IC) procedural guidance is available in Reference e. Additional DoD procedural guidance is available in References f-h.

RESPONSIBILITIES

6. The Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) shall:

a. Ensure Agency OCAs have a demonstrable and continuing need to exercise original classification authority;

b. Approve in writing requests to appropriate higher level authorities for *reclassifying* NSA/CSS information that has been declassified and released to the public under proper authority;

c. Authorize or delegate the authority to authorize the disclosure of *classified information* in *emergency situations* to individuals otherwise not eligible to receive the information;

d. Designate a *Senior Agency Official* to direct and administer NSA/CSS' *information security* program; and

e. Designate, at his/her discretion, a senior official to be responsible for overseeing *Special Access Programs* and *Controlled Access Programs* within NSA/CSS (see NSA/CSS Policy 1-41, -NSA/CSS Special Access Programs‖ (Reference n)).

7. The Associate Director for Policy and Records, as the Senior Agency Official, shall:

a. Perform the functions of component Senior Agency Official as outlined in References a, b, f, and h;

b. Serve as the NSA/CSS senior classification authority for classification and *declassification* guidance;

c. Grant, when appropriate, waivers to original and *derivative classification* training requirements;

d. Provide the final NSA/CSS determination on classification challenges. Inform the complainant of any right to appeal the decision to the Interagency Security Classification Appeals Panel (ISCAP) and the procedures for such an appeal; and

e. Remove original or derivative classification authority from those who show reckless disregard or a pattern of errors in applying the standards of References a-i or who have not received the required training. Notify the Information Security Oversight Office (ISOO) of violations as required in Section 5.5 of Reference a. Approve temporary waivers to the training requirements, as necessary.

8. The Associate Director for Policy and Records (ADPR, DJ) shall:

a. Establish uniform information security policies and procedures to ensure proper protection, handling, storage, and dissemination of all national security information under NSA/CSS purview or control;

b. Act as the NSA/CSS point of contact for all classification matters with the IC, DoD, and other departments or agencies, except for those addressed in Reference n (see Paragraph 16);

c. Interpret decisions concerning information security made by DIRNSA/CHCSS, the National Security Council, ISOO, the Secretary of Defense, the Office of the Director of National Intelligence (ODNI), and others as appropriate;

d. Establish and maintain classification and declassification policy in coordination with appropriate NSA/CSS stakeholder organizations to meet the information security needs of NSA/CSS;

e. Establish controls and procedures to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in Reference a, Section 4.1(a) in coordination with other appropriate NSA/CSS organizations with cognizance over or an equity in the information;

f. Oversee, in coordination with the Information Systems Security Risk Management Group, policies to require that classified information on information technology systems is collected, created, marked, used, communicated, computed, disseminated, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized individuals;

g. Establish and maintain NSA/CSS' ongoing information security *self-inspection* program;

h. Maintain and publish the list of authorized NSA/CSS OCAs;

i. Provide initial training to new OCAs prior to their exercising OCA responsibilities. This training shall cover, at a minimum, classification/declassification standards, classification levels, classification/declassification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, *classification guides*, and information sharing;

j. Provide all OCAs mandatory followup training in proper classification and declassification procedures at least once a calendar year;

k. Review for consistency and endorse all NSA/CSS classification and declassification proposals before they are forwarded to the appropriate OCA or

Declassification Authority for decision. This review and endorsement responsibility may be exercised by either the Associate Director or the Deputy Associate Director;

l. Manage the development of and maintain classification and *declassification guides* and ensure that *original classification* decisions are incorporated into classification guides on a timely basis in conjunction with appropriate NSA/CSS organizations with cognizance over or an equity in the information. Publish guides as necessary;

m. Establish procedures and conduct comprehensive evaluations to ensure that classification guides are regularly reviewed and updated at least once every 5 years;

n. Conduct the fundamental classification guidance review;

o. Establish and maintain the *Classification Advisory Officer (CAO) Program*;

p. Serve as the CAO for the Offices of the Director, General Counsel, Inspector General, and Chief of Staff organizations and for the Central Security Service (CSS) elements resident at NSA/CSS-Washington, if those elements do not have CAOs resident within their element;

q. Maintain and publish the list of NSA/CSS *Designated Intelligence Disclosure Officials (DIDOs)* and *Foreign Disclosure Officers (FDOs)*;

r. Establish and maintain an information security education and training program for all Agency affiliates;

s. Respond appropriately to requests for information, requirements, tasking, etc. from external organizations (e.g., the Secretary of Defense, the ODNI, ISOO, the CAPCO (Controlled Access Program Coordination Office), and ISCAP);

t. Ensure prompt and appropriate response to requests, appeals, challenges, complaints, and suggestions about NSA/CSS' information security program and policy;

u. Establish procedures to resolve allegations or complaints regarding overclassification or incorrect classification within NSA/CSS. Document procedures for classification and marking challenges in Policy Manual 1-52 (Reference k); and

v. Notify ADS&CI of any known or suspected unauthorized disclosure and/or compromise of classified information. Coordinate with ADS&CI in reporting security incidents involving the disclosure or compromise of classified information to appropriate higher level authorities.

9. NSA/CSS Original Classification Authorities (OCAs) shall:

a. Certify in writing to the NSA/CSS Senior Agency Official before initially exercising OCA authority and annually thereafter that they have received training on the

fundamentals of proper security classification and declassification, the limits of their authority, the sanctions that may be imposed, and OCA duties and responsibilities, as described in Paragraph 7.i. above. OCAs who do not receive such mandatory training at least once every calendar year shall have their original classification authority suspended;

b. Establish classification and declassification guides for the information, systems, plans, programs, projects, or missions involving NSA/CSS information over which they have program or management responsibility;

c. Validate the information in, update, or cancel the classification and declassification guides under their purview at least every 5 years or when directed as part of a fundamental classification guide review to ensure that the guides are current and accurate;

d. Respond with an answer or acknowledgement within 30 days of receipt to new requests for a classification determination for information under the OCA's purview from individuals who are not a cognizant OCA;

e. Raise or lower the classification level of or declassify NSA/CSS information under their purview as appropriate. For declassification decisions, determine whether public interest in disclosing information outweighs the damage to national security that might reasonably be expected from the disclosure of such information;

f. Recommend to DIRNSA/CHCSS, as appropriate, the *reclassification* of information that has been declassified and released to the public under proper authority;

g. Receive the endorsement of the ADPR or Deputy ADPR prior to making any original classification or declassification decisions. In a time-sensitive emergency situation, the OCA will advise DJ after the fact and complete any required records; and

h. Document all classification/declassification decisions in writing, e.g., in the form of a classification guide, memorandum, or other formal document.

10. NSA/CSS Classification Advisory Officers (CAOs) shall:

a. Meet eligibility and training requirements as specified by Information Security Policy (DJ2);

b. Provide guidance on protecting and marking national security information and classification matters pertinent to their organizations and area of expertise, consulting with other CAOs, subject matter experts, and Information Security Policy (DJ2) as necessary;

c. Assist in developing classification and declassification guides;

d. Perform initial classification review of NSA/CSS information intended for public dissemination, in accordance with NSA/CSS Policy 1-30, -Review of NSA/CSS Information for Public Dissemination‖ (Reference o);

e. Convey classification-related information and issues between their organizations and Information Security Policy (DJ2);

f. Assess the classification-related training needs of their organizations and assist Information Security Policy (DJ2) in providing the training;

g. Assist Information Security Policy (DJ2) with the NSA/CSS Self-Inspection Program;

h. Remain knowledgeable of NSA/CSS and higher level policies governing classification; and

i. Perform other duties as described in the -Memorandum on the NSA/CSS Classification Advisory Officer Program‖ (Reference p).

11. The NSA/CSS Chief of Staff, Directors, Associate Directors, and Extended Enterprise Commanders/Chiefs shall:

a. Establish procedures within their individual organization to facilitate information sharing, in accordance with NSA/CSS Policy 11-1, -Information Sharing‖ (Reference q), while still ensuring that access to classified information is limited to appropriately cleared personnel with a valid *need to know* (References a, f);

b. Establish CAO positions at appropriate organizational levels and in sufficient numbers to afford all members of their respective workforces ready access to necessary classification services;

c. Ensure that all employees under their authority receive mandatory information security training;

d. Ensure that all employees under their authority comply with the requirements of this policy and other relevant guidance; and

e. Develop and maintain classification and declassification guides and ensure that original classification decisions are incorporated into classification guides on a timely basis, in coordination with the Associate Director for Policy and Records.

12. The NSA/CSS Inspector General shall carry out audits and other evaluations as required by Public Law 111-258—Oct. 7, 2010, -Reducing Over-Classification Act‖ (Reference c).

13. The NSA/CSS Associate Director for Security and Counterintelligence (ADS&CI, Q) shall:

a. Review and, as appropriate, investigate instances of noncompliance with this policy that may constitute a security violation, in accordance with NSA/CSS Policy 5-2, "Security Investigations" (Reference r);

b. Coordinate with the Technology Director to resolve any incidents involving unauthorized access, compromise, or *data spills* of classified information resident in information systems; and

c. Report, in coordination with ADPR, security incidents involving the disclosure or compromise of classified information to appropriate higher level authorities and coordinate damage assessments specific to the compromise of classified information as appropriate.

14. The NSA/CSS Associate Director for Education and Training (ADET, E) shall collaborate with ADPR in mandatory and discretionary information security course development and delivery.

15. The Technology Director (TD) shall:

a. Establish, with information owners, uniform procedures that provide adequate protection to ensure automated information systems that collect, create, mark, use, communicate, compute, disseminate, process, store, reproduce, transmit, or destroy classified information:

1) Prevent access by unauthorized persons;

2) Ensure the integrity of the information; and

3) Use common standards and formats to maximize the availability of information to authorized users;

b. Provide, where feasible, an automated classification tool for NSA/CSS Enterprise Solutions-approved email client and standard office automation applications to assist the users with protecting information. It remains the responsibility of the user to ensure that the information is properly marked and safeguarded; and

c. Notify ADS&CI of any incidents involving unauthorized access, compromise, or data spills of classified information resident in information systems, and coordinate with ADS&CI as required to resolve the incident.

16. The SID Deputy Chief of Staff for Policy and Corporate Issues (S02) shall oversee the programs identified in Policy 1-41 (Reference n).

17. All NSA/CSS civilian and military personnel shall complete annual information security training. Civilian, military, contractor, and integree personnel working within NSA/CSS spaces and performing NSA/CSS mission but not assigned to NSA/CSS are encouraged but not required to receive this training.

18. Individuals applying derivative classification markings shall:

a. Observe and respect the classification determinations made by OCAs;

b. Use only authorized sources to make derivative classification decisions, such as classification guides, memorandums, or other forms of classification guidance formally issued by an OCA;

c. Explicitly and uniformly apply classification and control markings when creating, disseminating, or using classified NSA/CSS information to maximize information sharing while protecting sources, methods, and activities from unauthorized or unintentional disclosure;

d. Determine appropriate classification markings for the NSA/CSS information they produce and apply appropriate control markings that correctly implement DoD and ODNI guidelines for dissemination;

e. In accordance with applicable DoD and ODNI standards, portion mark all NSA/CSS documents that contain NSA/CSS information requiring control markings, regardless of classification, format, or medium;

f. Include a classification authority block on information that they derivatively classify, regardless of format or media. This must include a statement that appropriately identifies them as the derivative classifier of the information; and

g. Take all appropriate and reasonable steps, such as consulting a classification guide, requesting assistance from ADPR, or soliciting guidance from the appropriate OCA(s) or CAO(s) in cases where classification appears to be inconsistently or incorrectly applied. In cases of apparent conflict between a classification guide and a classified source document regarding a discrete item of information, the instructions in the classification guide shall take precedence.

19. The supervisors of all civilian personnel whose duties include significant involvement with creating or handling classified information shall include in the performance assessment of these individuals an evaluation of their marking and management of classified information.

20. All authorized holders of NSA/CSS information shall:

a. Be held personally and individually responsible for properly safeguarding NSA/CSS classified national security information under their custody and control;

b. Complete annual information security refresher training compliant with DoD and ODNI requirements;

c. Ensure that access to such information is granted only to individuals with the appropriate clearances and accesses and a valid need to know;

d. Indicate, through marking or other means, the portions of national security information that require protection as classified and the portions that do not;

e. When practicable, use a classified addendum whenever classified information constitutes a small portion of a document that is otherwise not classified;

f. Challenge the classification status of information they believe is improperly or incorrectly classified;

g. Ensure that classified information is not removed from official premises without proper authorization and approved safeguards;

h. Take custody of and safeguard classified material that is not properly controlled. Immediately notify ADS&CI;

i. Immediately notify ADS&CI upon the loss, unauthorized disclosure, or potential compromise of classified information;

j. Comply with the prepublication review processes specified in Reference o;

k. Not remove classified information from the Agency's control or direct that information be declassified to remove it from Agency control when leaving Agency service; and

l. Attend a termination briefing when leaving Agency service that emphasizes their continued responsibility to protect national security information to which they have had access.

REFERENCES

21. References:

a. Executive Order 13526, -Classified National Security Information,‖ dated 29 December 2009.

b. ISOO, -ISOO Implementing Directive for E.O. 13526, 32 CFR Parts 2001 and 2003,‖ dated 28 June 2010.

c. Public Law 111-258—Oct. 7, 2010, -Reducing Over-Classification Act.‖

d. Intelligence Community Directive (ICD) 700, -Protection of National Intelligence,‖ dated 21 September 2007. (On Intelink at http://www.intelink.ic.gov/sites/ppr/policyHome/ICD/ICD_700 /default.aspx)

e. ICD 710, -Classification and Control Markings System,‖ dated 11 September 2009. (On Intelink at http://www.intelink.ic.gov/sites /ppr/policyHome/ICD/ICD_710/default.aspx)

f. Department of Defense Manual (DoDM) 5200.01, Volume 1, -DoD Information Security Program: Overview, Classification, and Declassification ,‖ dated 24 February 2012.

g. DoDM 5200.01, Volume 2, -DoD Information Security Program: Marking of Classified Information,‖ dated 24 February 2012.

h. DoDM 5200.01, Volume 3, -DoD Information Security Program: Protection of Classified Information,‖ dated 24 February 2012.

i. Executive Order 13587, -Structural Reform to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,‖ dated 13 October 2011.

j. Atomic Energy Act of 1954, as amended (Public Law 83-703).

k. NSA/CSS Policy Manual 1-52, -NSA/CSS Classification Manual,‖ dated 23 November 2004, revised 8 January 2007.

l. Executive Order 12333, -United States Intelligence Activities,‖ as amended.

m. DoD Directive 5100.20, -The National Security Agency and Central Security Service,‖ dated 26 January 2010.

n. NSA/CSS Policy 1-41, -NSA/CSS Special Access Programs,‖ dated 29 September 2005.

o. NSA/CSS Policy 1-30, -Review of NSA/CSS Information for Public Dissemination,‖ dated 15 December 2004, revised 9 January 2012.

p. -Memorandum on the NSA/CSS Classification Advisory Officer Program,‖ dated 21 June 2010.

q. NSA/CSS Policy 11-1, -Information Sharing,‖ dated 28 March 2012.

r. NSA/CSS Policy 5-2, -Security Investigations, ‖ dated 16 December 2003.

DEFINITIONS

22. Affiliate – A person employed by, detailed to, or assigned to NSA/CSS, including members of the U.S. Armed Forces; consultants to NSA/CSS; industrial or commercial contractors, licensees, certificate holders, or grantees of NSA/CSS, including all subcontractors; personal services contractors, foreign partners detailed to NSA/CSS; or any other category of person who acts for or on behalf of NSA/CSS as determined by DIRNSA/CHCSS. (Source: Adapted from NSA/CSS Policy 5-15)

23. Classifying – The act or process by which information is determined to be classified information (Reference a).

24. Classification Advisory Officer (CAO) Program – An NSA/CSS-unique program, administered by Information Security Policy (DJ2), for training and certifying individuals who are responsible for ensuring that classified and sensitive information in their organizations is properly marked and protected and that the employees in their organizations understand and properly apply classification rules and guidance.

25. Classification Guide – A documentary form of classification guidance issued by an Original Classification Authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element (Reference a).

26. Classified Information – See Classified National Security Information.

27. Classified National Security Information – Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form (Reference a).

28. Controlled Access Programs – Programs established to protect extremely sensitive and critical intelligence information; these include *Sensitive Compartmented Information* (SCI) (Reference n).

29. Controlled Unclassified Information – Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. (Source: DoDM 5200.01, Vol. 4)

30. Data Spill – When information of a higher classification escapes (advertently or inadvertently) to a system of a lower classification.

31. Declassifying – The authorized change in the status of information from classified information to unclassified information (Reference a).

32. Declassification Authority – The official who authorized the original classification if that official is still serving in the same position, the originator's current successor in function if that individual has original classification authority, a supervisory official of either the originator

or his or her successor in function if the supervisory official has original classification authority, or officials delegated Declassification Authority in writing by DIRNSA/CHCSS or the Senior Agency Official. An NSA/CSS OCA also acts as the Declassification Authority for information under his or her purview (Reference f).

33. Declassification Guide – Written instructions issued by a Declassification Authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified (Reference a).

34. Derivative Classification – Incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification (Reference a).

35. Designated Intelligence Disclosure Officials (DIDOs) – Heads of United States Government agencies and departments within the Intelligence Community, their specifically designated subordinates, and other United States officials designated by the Director of Central Intelligence. (Source: Derived from NSA/CSS Policy 1-53)

36. Downgrade – A determination by a Declassification Authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level (Reference a).

37. Emergency Situation – Circumstances in which there is an imminent threat to life or in defense of the homeland (Reference h).

38. Foreign Disclosure Officers (FDOs) – Officials, specifically designated in writing, who may disclose or deny classified military information in accordance with the provisions of the National Disclosure Policy, provided that the information is originated by the official's department or agency and that the official is responsible for the information to be disclosed. Only those officials with specific authority may make foreign disclosure determinations. (Source: NSA/CSS Policy 1-53)

39. Information – Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government (Reference a).

40. Information Security – The system of policies, procedures, and requirements established in accordance with Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to the provisions of the Freedom of Information Act (Reference f).

41. Need to Know – A determination within the executive branch in accordance with directives issued pursuant to Executive Order 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function (Reference a).

42. Original Classification – The initial determination that information requires, in the interests of national security, protection against unauthorized disclosure (Reference a).

43. Original Classification Authority (OCA) – An individual authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to classify information in the first instance (Reference a).

44. Reclassifying – Classifying information that had been previously declassified and released under proper authority. (Source: Derived from Reference a)

45. Safeguarding – Measures and controls that are prescribed to protect classified information (Reference a).

46. Self-inspection – The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under Executive Order 13526 and its implementing directives (Reference a).

47. Senior Agency Official – The official appointed to be responsible for directing and administering the Agency's program under which information is classified, safeguarded, and declassified. (Source: Derived from Reference a) Note: The Associate Director for Policy and Records is the NSA/CSS Senior Agency Official.

48. Sensitive Compartmented Information – Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established and overseen by the Director of National Intelligence. (Source: ICS Number 2008-700-1)

49. Special Access Program – A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (Source: DoDD 5205.07)

50. Unauthorized Disclosure – Communication or physical transfer of classified information to an unauthorized recipient (Reference a).