(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 12/13/2010

To: CJIS Attn: Global Operations Section
Global Initiatives Unit,
Module C-3
UC [redacted] b6
SSA [redacted] b7C
MPA [redacted] b7E

International Operations Attn: [redacted]
UC [redacted]
SSA [redacted]
FOS [redacted]

From: [redacted]
Legal Attache (Legat) Office
Contact: Legat [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] ~~(Pending)~~ b3
[redacted] ~~(Pending)~~ b7A
b7E

Title: [redacted] b7E

Synopsis: Biometrics Memorandum of Cooperation (MOC) Success.

Reference: [redacted] b3
b7E

UNCLASSIFIED

To: CJIS From: [redacted]
Re: [redacted] 12/13/2010 b3 b7E

Enclosure(s): Enclosed for the Criminal Justice Information Services (CJIS) Division is one copy each of the original, signed, English-language and Arabic-language *MEMORANDUM OF COOPERATION between THE UNITED STATES FEDERAL BUREAU OF INVESTIGATION and THE IRAQ MINISTRY OF INTERIOR regarding EXCHANGE OF BIOMETRIC IDENTIFICATION INFORMATION*. The sole duplicate-original was filed at the Government of Iraq (GOI), Ministry of Interior (MOI), on 12/12/2010.

Details: As set out in referenced [redacted] on 06/18/2009 a proposal was made to Iraqi Interior Minister Jawad al-Bolani recommending the development of a memorandum of cooperation (MOC) between the Iraqi MOI and the United States (U.S.) Federal Bureau of Investigation (FBI), to exchange biometric identification information pertaining to law enforcement matters. Minister Bolani indicated that he was favorably disposed toward the idea, and an effort was undertaken by MOI personnel, the FBI CJIS Division's Global Initiatives Unit (GIU), and Legat [redacted] to craft a mutually acceptable MOU. b3 b7E

Attorneys and executive management within both the MOI and FBI reviewed and fine-tuned several draft MOCs, and during October 2010, the GOI proposed a final draft document which had been approved by the Iraqi Interior Minister, the Prime Minister, and the Counsel of Ministers. The final draft was reviewed and approved by the FBI's Office of the General Counsel (OGC), and by CJIS and International Operations Division (IOD) executive management. [The English-language copy has two minor typographical errors which FBI counsel deemed immaterial in approving the enclosed version of the MOC for final signature, to wit: CJIS Assistant Director (AD) Daniel D. Roberts was incorrectly identified as the "Acting Assistant Director;" and Legat [redacted] was incorrectly referred to as [redacted] b6 b7C

The GOI deemed the appropriate signatory to be Iraqi Police (IP) Lieutenant General (LTG) Iyden Khalid Kadir, Deputy Minister for Police Affairs. The FBI deemed AD Roberts and Legat [redacted] to be the appropriate signatories on behalf of the FBI. b6 b7C

On 10/17/2010, LTG Iyden (sometimes transliterated "Ayden") signed the MOC. Legat [redacted] affixed his signature on 10/20/2010. AD Roberts signed on 10/29/2010, at which time the MOC went into effect on the U.S. Government side. However, the GOI did not consider the document effective until an original copy was filed at the MOI on 12/12/2010. b6 b7C

It should be noted here that [redacted] the U.S. Embassy [redacted] was absolutely essential in ensuring that the GOI came to b6 b7C b7E

To: CJIS From: [redacted]
Re: [redacted] 12/13/2010 b3 b7E

an agreement with the FBI on this matter, and he further ensured that the GOI was meticulous in obtaining necessary approvals from the Prime Minister and the Counsel of Ministers. [redacted] b6 b7C

[redacted]

Similarly, [redacted] b6 b7C b7E

[redacted] was an essential partner in successfully concluding the MOC. [redacted] works directly with Colonel Ali Obaid Abbas, Director of [redacted]

There remain significant challenges in executing the signed MOC. Legat [redacted] remains committed to meeting the challenges. b7E

To: CJIS From: [redacted]
Re: [redacted] 12/13/2010

b3
b7E

LEAD(s):

Set Lead 1: (Action)

CJIS

AT CLARKSBURG, WV

The CJIS Global Initiatives Unit (GIU) is requested to file the enclosed original documents, as appropriate.

Set Lead 2: (Info)

INTERNATIONAL OPERATIONS

AT INTERNATIONAL FUSION CELL

Read and clear.

◆◆

[Intentionally Inserted to Denote Separate Documents]

U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

FBI CJIS Division
Policy for Biometric Information Sharing With Domestic and International Agencies

Prepared by:
Global Operations Section
Interoperability Initiatives Unit
November 24, 2010

FBI CJIS Division Policy for Biometric Information Sharing With Domestic and International Agencies

1. Policy Title

FBI CJIS Division Policy for Biometric Information Sharing with Domestic and International Agencies

2. Authorities

a. 5 U.S.C. § 552a, as amended (Privacy Act of 1974)
b. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001
c. The Homeland Security Act of 2002
d. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004
e. Executive Order 13388 of October 25, 2005, Further Strengthening the Sharing of Terrorism Information to Protect Americans
f. Homeland Security Presidential Directive (HSPD) 2
g. HSPD 6
h. HSPD 11
i. National Security Presidential Directive (NSPD) 59 / HSPD 24

3. Purpose

The purpose of this policy is to establish the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division's standardized approach to biometric information sharing with domestic and international agencies for the administration of criminal justice or national security purposes. Establishment of this policy will provide the ability for enhanced record sharing and improved person-centric identification across the United States Government (USG) and with international partners. This policy will ensure that the disclosure of information is compatible with the purpose for which the information was collected; information is related to the Sharing Partners responsibilities; is in direct correlation to the FBI's mission; and is in compliance with the CJIS Advisory Policy Board (APB) Data Protection Strategies. Dependent upon the method by which the biometric information sharing initiative will be accomplished, this policy will also ensure the records shared are complete, accurate, timely and relevant.

Information sharing activities accomplished through the Integrated Automated Fingerprint Identification System (IAFIS)/NGI are exempt from the FBI Information Sharing Activities with Other Government Agencies policy (Corporate Policy Directive 0012D). Implementation of this policy will support the FBI's roles and responsibilities for implementation of NSPD 59 / HSPD 24, while establishing policy to address other FBI CJIS Division records and recommended methods of sharing.

4. Policy Statement

To establish a policy for the FBI CJIS Division covering biometric information sharing with a domestic or international agency:

a. The FBI CJIS Division will establish a Biometric Information Sharing Working Group (BISWG) to consist of subject matter experts from across the CJIS Division and the data owners to ensure all potentially impacted areas are informed of biometric information sharing initiatives and have the opportunity to discuss impacts and risks prior to the BISWG's decision.
b. A Biometric Information Sharing Checklist will document the criteria requirements necessary to determine what information can be shared with a domestic or international agency. The category of records (e.g., Wanted Persons, Sexual Offender Registry), associated biometrics (e.g., fingerprints, latents, palmprints) and biographics (e.g., name, date of birth, gender) will be determined on a case by case basis.
c. These agreements will be discussed through the BISWG and documented in accordance with 4(g) or (h).
d. The FBI CJIS Division will pursue obtaining comparable categories of biometric records from the domestic or international agency with all biometric information sharing initiatives.

e. The FBI CJIS Division will exchange the biometrics and biographics using the following methods in order of preference:
    i. If connectivity exists between the FBI CJIS Division's biometric repository and the domestic or international agency, the FBI CJIS Division will perform biometric exchange in an automated manner via shared services. For domestic or international agencies with a defined business need, this method of sharing will provide a means of access to search the FBI CJIS Division's full biometric repository.
    ii. If connectivity exists between the FBI CJIS Division's biometric repository and the domestic or international agency and circumstances exist where a shared services methodology will not satisfy the requirements of the domestic or international agency, a shared data methodology may be used. This method will allow authorized records to be shared automatically through the existing connection with near-real time maintenance being performed to ensure data accuracy and integrity.
    iii. If connectivity does not exist, the FBI CJIS Division will determine the feasibility of establishing a connection.
    iv. If connectivity does not exist and it is determined a connection will not be established, the records will be considered for sharing via an extract. Approval for this method of sharing and all associated processing requirements will be determined and approved on a case-by-case basis through the BISWG.
f. The FBI CJIS Division will pursue the establishment of written governing document(s), such as an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or Memorandum of Cooperation (MOC) with the domestic or international agency to control biometric information sharing initiatives.
g. Written governing documents must cover specifics associated with the biometric information sharing initiative to include, but not limited to:
    i. Categories of records and associated biographics included in the biometric sharing initiative
    ii. Method by which the records will be exchanged
    iii. Method by which notifications will be exchanged (if applicable)
    iv. Data Maintenance
    v. Data Retention
    vi. Restrictions on the Use and Disclosure of Information
    vii. Third Party Dissemination
    viii. Data Disposal
    ix. Data Security
    x. Redress
h. In the event that the FBI CJIS Division cannot satisfy the condition to establish jointly-held written governing documents, the Biometric Information Sharing Checklist will be considered the governing document for the biometric sharing initiative.
i. The FBI CJIS Division sharing initiative point of contact will assess the need to conduct a Privacy Threshold Analysis and/or Privacy Impact Assessment for each biometric sharing initiative and mark the checklist accordingly.
j. The FBI CJIS Division sharing initiative point of contact will clearly communicate existing biometric sharing procedures and protocols with the domestic or international agency to address how records exchanged from domestic or international agencies will be shared across agencies.
k. Information from the Federal Identification Records System (FIRS), retained within the domestic or international biometric repository shall not be further disseminated in a manner that would violate Federal law, regulation, relevant APB Data Protection Strategies or applicable System of Records Notices. This may require the FBI CJIS Division to obtain from the domestic or international agency full disclosure on:
    i. Agencies accessing/searching the data within the respective system;
    ii. Dissemination rules/notifications procedures when hits occur.

5. Scope

This policy applies to all FBI CJIS Division Sections involved with activities related to biometric information sharing initiatives with domestic or international agencies.

6. Roles and Responsibilities

A Charter has been established to further define the roles and responsibilities of the BISWG. The remainder of this section provides high level responsibilities.

a. The FBI CJIS Division shall:
   i. Establish a point of contact for each biometric information sharing initiative;
   ii. Identify the liaison with the domestic or international agency;
   iii. Pursue establishment of jointly-held written governing documents;
   iv. Complete necessary documentation to be maintained by the Biometric Information Sharing Working Group when jointly-held written governing documents cannot be established.

b. The FBI CJIS Division BISWG shall:
   i. Review and assess all biometric information sharing initiatives, including all information provided by the established point of contact.
   ii. Maintain documentation or access to documentation, on all biometric information sharing initiatives.
   iii. Discuss biometric sharing initiatives and when necessary involve other substantive FBI units or boards (e.g., Counterterrorism Division, Full APB/Compact Council) and determine approval.

7. Exemptions

a. Sharing initiatives prior to October 1, 2010 are exempt from this policy. Renewals of any such policies will be subject to this policy.
b. Sharing initiatives concerning FBI owned records that are approved by the AD and/or DAD are exempt from this policy. However, a Biometric Information Sharing Checklist should be provided to the BISWG for tracking purposes only and written notification of the AD and/or DAD decision.
c. Under rare circumstances, the CJIS Division may receive an expedited request for records (i.e., Flyaway mission, natural disaster). When time does not permit for a BISWG meeting to occur, these types of requests can be approved by the AD and/or DAD. However, the POC for the record sharing initiative is required to provide a follow-up briefing to the BISWG and complete a Biometric Information Sharing Checklist documenting the records shared and the AD and/or DAD decision.

8. References

a. References
   i. 5 U.S.C. § 552a, as amended (Privacy Act of 1974)
   ii. USA PATRIOT Act of 2001, as amended in 2005
   iii. The Homeland Security Act of 2002, as amended by IRTPA of 2004
   iv. Executive Order 13388 of October 25, 2005, Further Strengthening the Sharing of Terrorism Information to Protect Americans
   v. HSPD 2
   vi. HSPD 6
   vii. HSPD 11
   viii. NSPD 59 / HSPD 24
   ix. Corporate Policy Directive, dated May 14, 2009, Proper Handling and Protection of Personally Identifiable Information on Mobile Devices
   x. CJIS Advisory Policy Board (APB) Data Protection Strategies

9. Definitions

a. Administration of Criminal Justice – detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

b. Shared Services – ability for each agency to submit fingerprint transactions to the other agency for a search of that agency's complete repository, allowing each agency to follow internal guidelines and policies for response dissemination and hit notifications. Mechanism by which biometric information sharing is accomplished via searches of a domestic or international biometric repository.

c. Shared Data – ability for authorized records to be shared automatically through an existing connectivity with near-real time maintenance being performed to ensure data accuracy and integrity.

d. Extract – a bulk set of records removed from a repository and provided to another agency for information sharing purposes.

10. Appendices, Attachments, and Forms

Biometric Information Sharing Checklist
Biometric Information Sharing Working Group Charter

[Intentionally Inserted to Denote Separate Documents]

U.S. Department of Justice

Federal Bureau of Investigation

United States Embassy
[redacted] b7E

April 2, 2011

Ministry of Interior
[redacted]

Attention: Deputy Minister of Interior
Lt. Gen. Ayden Khalid Qader

Dear Deputy Minister Ayden,

The Federal Bureau of Investigation greatly values its partnership with the Ministry of Interior in working toward our shared goal of defeating terrorism and transnational crime. An important step toward that goal has been the memorandum of cooperation on the exchange of biometric data, which went into effect on October 29, 2010. The Federal Bureau of Investigation appreciates your strong support for the memorandum and its subsequent approval by the Council of Ministers.

Under the terms of that memorandum, the United States [redacted] are now ready to begin b7E
exchanging fingerprint records of individuals who may be involved in terrorist activities, serious crime, or transnational activities threatening to national security. It is expected that this will be an ongoing, mutual exchange of biometric data that are not subject to dissemination restrictions under laws, regulations, and policies of [redacted] the United States.

In accordance with the memorandum, the Legal Attaché office is requesting the Ministry of Interior to begin exchanging fingerprints at this time with our office on a regular basis. We encourage the Ministry of Interior to identify categories of data they would be interested in receiving. This exchange will include known fingerprint records as well as requests for checks of unidentified fingerprints. Until an electronic connection can be established for transmission of data, fingerprints can be exchanged on CD-ROM, or in paper copy if necessary, with the Legal Attaché office.

To promote effective and consistent data sharing, Colonel Abbas Ali Ubayd has requested that the Federal Bureau of Investigation provide biometrics training to his personnel. This training, provided by specialists who administer the Integrated Automated Fingerprint Identification System of the Federal Bureau of Investigation, would tentatively be held May 2-5, 2011, at [redacted] We b7E
therefore request your approval to provide this training to approximately 25 personnel.

The Federal Bureau of Investigation appreciates your support of this biometrics partnership. As always, if the Federal Bureau of Investigation can be of assistance to you and the Ministry of Interior, please do not hesitate to ask.

[redacted] b6 b7C

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

[redacted] b3 b7E

وزارة العدل الأمريكية

مكتب التحقيقات الفدرالي

سفارة الولايات المتحدة

[redacted] b7E

2 نيسان 2011

وزارة الداخلية

[redacted]

إلى سعادة وكيل وزارة الداخلية
سيادة الفريق آيدن خالد قادر

سعادة وكيل الوزارة الفريق آيدن المحترم،

يثمن مكتب التحقيقات الفدرالي شراكته المتينة مع وزارة الداخلية عاليا من اجل العمل معا نحو هدفنا المشترك في دحر الإرهاب والجريمة العابرة للحدود. وان إحدى الخطوات المهمة نحو هذا الهدف بالتأكيد هي مذكرة التعاون لتبادل البيانات البيومترية، والتي دخلت حيز التنفيذ في 29 تشرين الأول 2010. ويقدر مكتب التحقيقات الفدرالي دعمكم الراسخ للمذكرة وبالتالي الموافقة عليها من قبل مجلس الوزراء.

إن الولايات المتحدة [redacted] في ظل شروط تلك المذكرة مستعدين حاليا للبدء بتبادل سجلات بصمات الأصابع للأشخاص الذين يحتمل ضلوعهم في النشاطات الإرهابية والجرائم الخطيرة والنشاطات العابرة للحدود والتي تهدد الأمن القومي. ومن المتوقع أن تستمر تبادل هذه البيانات البيومترية المشتركة وان لا تخضع إلى القيود المفروضة على التعميم بموجب القوانين والأنظمة وسياسات [redacted] الولايات المتحدة. b7E

يرجوا مكتب الملحق القانوني، وفقا للمذكرة، من وزارة الداخلية لتبدأ في هذا الوقت بتبادل بصمات الأصابع مع مكتبنا بصورة منتظمة ونشجع وزارة الداخلية على تحديد أصناف البيانات التي يرغبون في استلامها. ولتتضمن هذا التبادل سجلات بصمات الأصابع المعروفة بالإضافة إلى طلبات التدقيق في بصمات الأصابع الغير معروفة. والى أن يتم تأسيس اتصال الكتروني لنقل البيانات، يمكن أن يتم تبادل بصمات الأصابع مع مكتب الملحق القانوني بواسطة أقراص السي دي رام أو عن طريق نسخة ورقية إذا دعت الضرورة.

من اجل تعزيز تبادل البيانات بصورة فعالة ومستمرة، طلب العقيد عباس علي عبيد أن يقوم مكتب التحقيقات الفيدرالي بفتح دورة تدريبية للبيانات البيومترية للموظفين العاملين عنده. وان هذه الدورة التدريبية، والتي يتم تزويدها من قبل المختصين الذين يشرفون على البرنامج التلقائي الموحد للتعرف على بصمات الأصابع التابعة لمكتب التحقيقات الفيدرالي، مدرج في الجدول للانعقاد في [redacted] من 2 إلى 5 آيار من عام 2011. b7E

ويقدر مكتب التحقيقات الفيدرالي جهودكم المستمرة لدعم هذه الشراكة البيومترية. وكما هو الحال دائما، فإن مكتب التحقيقات الفيدرالي مستعد لتلبية طلبكم للمساعدة إذا كنتم في حاجة إليها و نرجو أن لا تترددوا في طلب كهذا وشكرًا لكم.

[redacted] b6 b7C

[Intentionally Inserted to Denote Separate Documents]

b6
b7C

~~SECRET//NOFORN~~
(U)

(U) Foreign Dissemination of Unclassified Information

(U) Policy Directive and

(U) Policy Guide

(U) Federal Bureau of Investigation

(U) National Security Branch

(U) 0580DPG

(U) Published Date: April 20, 2013

(U) Review Date: May 24, 2017

(U)
~~Classified By: [redacted]~~
~~Declassify On: 20380103~~
~~Derived From: FBI NSISC-20120727~~

b6
b7C

Note: This document incorporates the policy directive and the policy guide.

~~SECRET//NOFORN~~
(U)

5. (U) Policies and Procedures for Unclassified Information Sharing with Foreign Recipients

5.1. (U) Foreign Sharing: Guiding Principles for Sharing Unclassified Information with a Foreign Recipient

(U) Author/holders of the unclassified information cannot guarantee that the foreign recipient will safeguard the information from future disseminations once it is in the foreign recipient's possession. Therefore, author/holders must follow the instructions in this PG to assure that unclassified information is disseminated to countries that will protect the information.

(U//~~FOUO~~) It is a violation of FBI policy and security regulations for any FBI employee (including task force officers, contractors, and detailees) to share unclassified information with a foreign government, unless the sharing of information is within the employee's official duty.

(U//~~FOUO~~) Before any decision is made to share unclassified information with a foreign recipient, the FBI employee must take into account the expected risks, such as:

- (U//~~FOUO~~) Whether the information will be further disseminated to another government or any other party without the approval of the originating U.S. department or agency.
- (U//~~FOUO~~) Whether the information will be used for reasons other than the stated purpose and will likely to be used by the foreign government in a manner harmful to U.S. interests.

(U//~~FOUO~~) The FBI may pass unclassified information to foreign recipients only if:

- It is required by statutes or treaties, EOs, Presidential directives, National Security Council directives, Homeland Security Council directives, and AG-approved policies, memoranda of understanding, or agreements.; or
- The dissemination is related to the foreign agency's responsibilities, is consistent with U.S. interests, the FBI has considered the effect of such dissemination may have on any identifiable USPER, and the purpose of the dissemination is compatible with the purpose for which the information was collected.

5.2. (U) Presenting FBI Information to a Foreign Recipient

(U//~~FOUO~~) When disclosing information to a foreign recipient in an oral presentation, it is the responsibility of the presenter to make sure the classification and foreign release markings adequately safeguard the information, including the medium used to disclose the information.

5.3. (U) Human Rights

(U//~~FOUO~~) If uncertain of a government's human rights practices, author/holders of the information to be disseminated must review the most recent Country Reports on Human Rights before approving dissemination. In addition, author/holders may contact IOD regional unit and other federal agencies in determining human rights practices of potential recipient countries. The annual Country Reports on Human Rights are

administered and published by the Department of State and can only be accessed from the Internet.

5.4. (U) Dissemination Control Markings for Unclassified Information

(U) Information marked "UNCLASSIFIED" without any warning statements or caveats is subject to be further disseminated without the originating operational division's or FO's consent.

(U) Authors/holders must apply a control marking such as For Official Use Only (~~FOUO~~); Law Enforcement Sensitive (LES); or LES Not Releasable to Foreign Recipients (LES NOFORN) when the information meets the appropriate standards for use of such marking.

(U) Unclassified dissemination control markings are applied at the discretion of the FBI employee following guidelines contained in the Intelligence Community Authorized Classification and Control Markings Register and Manual.

5.4.1. (U) Dissemination Control Markings for Unclassified Information marked FOUO, LES, or LES NOFORN

(U) The most common dissemination control markings used by the FBI for unclassified information are FOUO, LES, and LES NOFORN.

- (U) UNCLASSIFIED: Authors/holders of information that is marked "UNCLASSIFIED" (without any dissemination control markings or warning statements/caveats) may disseminate the information to foreign recipients, after appropriate legal review (in accordance with the policies set forth in Section 3 of this PG), without permission of the originating operational division or FO.
- (U) ~~FOUO~~: Authors/holders of Unclassified information marked as "FOUO" may disseminate the information to foreign recipients, after appropriate legal review (in accordance with the policies set forth in Section 3 of this PG), without permission of the originating operational division or FO.
- (U//~~FOUO~~) LES: Authors/holders of unclassified information marked as "LES" may disseminate the information to foreign recipients, after appropriate legal review (in accordance with the policies set forth in Section 3 of this PG), with permission of the originating operational division or FO.
- (U//~~FOUO~~) LES NOFORN: Authors/holders of unclassified information marked as "LES NOFORN" may not disseminate the information to any foreign recipient.

(U) All unclassified information containing LES or LES NOFORN must contain an appropriate standard warning statement (or a version edited to limit or expand dissemination or to show information origination), as specified in the *Law Enforcement Sensitive Information Policy Directive and Policy Guide* (0736DPG).

(U) As of December 2011, the following dissemination control markings used for classified information are now authorized by Controlled Access Program Coordination Office (CAPCO) for use with unclassified information[5]:

[5] (U//~~FOUO~~) *Intelligence Community Authorized Classification and Control Markings Register and Manual*, Volume 5, Edition 1 (Version 5.1) - REL TO page 114; RELIDO page 118; and NOFORN page 110.

- Authorized for Release To (REL TO): Information may only be disseminated to the country or countries specified without further approval by the originator. Dissemination to all other countries is prohibited unless the originator grants approval.
- Not Releasable to Foreign Nationals (NOFORN): Information may not be released in any form to foreign recipients, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.
- Originator Controlled (ORCON): Information may only be disseminated within the recipient organization's headquarters and specified subordinate elements; however, the recipient organization may not further disseminate the information outside itself without advanced permission from the originator.

(U//~~FOUO~~) Author/holders should consult the *Intelligence Community Authorized Classification and Control Markings Register and Manual* for a comprehensive list of authorized unclassified control markings and the authority for each.
(U//~~FOUO~~) For additional guidance on classification and new unclassified markings, refer to the Security Division Information Security Team's National Security Information Program Intranet site or the Controlled Unclassified Information (CUI) Program Intranet site.
(U) EO 13556, titled "Controlled Unclassified Information" directed the establishment of a government-wide standard for unclassified information requiring safeguarding measures or dissemination controls, which will be called Controlled Unclassified Information. Until the new Controlled Unclassified Information marking is approved to be used by the Intelligence Community, Controlled Unclassified Information is not authorized for use as an unclassified marking.

5.4.2. (U) Other Markings

(U//~~FOUO~~) For guidance on other Intelligence Community markings, consult the Controlled Access Program Coordination Office's *Intelligence Community Authorized Classification and Control Markings Register and Manual*, or contact any of the individuals listed on SecD's Information Security-National Security Information Program Intranet page.