DEFENSE

Security of Information

Agreement between
the UNITED STATES OF AMERICA
and JAPAN

Signed at Tokyo August 10, 2007

with

Annex
NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966
(80 Stat. 271; 1 U.S.C. 113)—

“. . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof.”
JAPAN

Defense: Security of Information

AGREEMENT BETWEEN THE GOVERNMENT OF
THE UNITED STATES OF AMERICA AND THE GOVERNMENT OF JAPAN
CONCERNING SECURITY MEASURES FOR
THE PROTECTION OF CLASSIFIED MILITARY INFORMATION

Preamble

The Government of the United States of America and the Government of Japan (hereinafter referred to as "the Parties" and separately as "a Party"),

Affirming that the United States-Japan security arrangements, based on the Treaty of Mutual Cooperation and Security between the United States of America and Japan signed at Washington on January 19, 1960, is the cornerstone for achieving common security objectives,

Recognizing that the Mutual Defense Assistance Agreement between the United States of America and Japan signed at Tokyo on March 8, 1954, and the arrangements made thereunder have provided for the reciprocal exchange of defense-related information,

Recalling that, at the meeting of the Security Consultative Committee on October 29, 2005, the Ministers expressed their commitment to take additional necessary measures to protect shared classified information so that broader information sharing is promoted among pertinent authorities,

Desiring to further mutual cooperation to ensure the protection of classified military information;

Have agreed as follows:

Article 1
Definitions

For the purposes of this Agreement,

(a) "Classified Military Information" (hereinafter referred to as "CMI") means any defense-related information that is generated by or for the use of or held by the Department of Defense of the United States of America or the Ministry of Defense of Japan, or defense-related information generated by or for the use of or held by other relevant authorities of the Government of the United States of America or the Government of Japan, and that requires protection in the interests of national security of the originating
Party. The information shall bear a security classification and, where necessary, an appropriate indication to identify such information as CMI. Such information may be in oral, visual, electronic, magnetic, or documentary form, or in the form of equipment or technology;

(b) "national laws and regulations" means,

(i) in relation to Japan, the laws listed in the Annex attached hereto and other relevant laws and regulations, and

(ii) in relation to the United States of America, the laws that will be notified by the Government of the United States of America to the Government of Japan through diplomatic channels and other relevant laws and regulations;

(c) "personnel security clearance" means an eligibility for handling securely CMI granted to individuals in accordance with each Party's appropriate procedures.

Article 2
Protection of CMI

CMI provided directly or indirectly by one Party to the other Party shall be protected under the terms set forth herein, provided that they are consistent with the national laws and regulations of the recipient Party.

Article 3
Changes in National Laws and Regulations

Each Party shall notify the other of any changes to its national laws and regulations that would affect the protection of CMI under this Agreement. In such case, the Parties shall consult, as provided for in Article 19(b), to consider possible amendments to this Agreement. In the interim, CMI shall continue to be protected in accordance with the provisions of this Agreement, unless otherwise approved in writing by the releasing Party.

Article 4
Security Classification and Marking of CMI

For the Government of the United States of America, CMI shall be marked Top Secret, Secret, or Confidential. For the Government of Japan, CMI that is designated as "Defense Secret" according to the Self-Defense Forces Law
shall be marked "Bouei Himitsu," and the other CMI that is not designated as "Defense Secret" shall be marked "Kimitsu," "Gokuhi," or "Hi" depending on the sensitivity of the information concerned.

"Bouei Himitsu" that bears the additional marking "Kimitsu" shall be afforded a degree of protection equivalent to United States "Top Secret." "Bouei Himitsu" shall be afforded a degree of protection equivalent to United States "Secret."

Equivalent classifications shall be as follows:

<table>
<thead>
<tr>
<th>United States of America</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Secret</td>
<td>Kimitsu 機密</td>
</tr>
<tr>
<td></td>
<td>/Bouei Himitsu(Kimitsu) 防衛秘密 (機密)</td>
</tr>
<tr>
<td>Secret</td>
<td>Gokuhi 極秘</td>
</tr>
<tr>
<td></td>
<td>/Bouei Himitsu 防衛秘密</td>
</tr>
<tr>
<td>Confidential</td>
<td>Hi 秘</td>
</tr>
</tbody>
</table>

Each recipient Party shall stamp or mark the name of the releasing Party on all CMI. The CMI shall also be marked with the equivalent security classification of the recipient Party.

Article 5
Supplemental Implementing Arrangements

Supplemental implementing arrangements under this Agreement may be entered into by competent authorities of the Parties. For the Government of the United States of America, the competent authority shall be the Department of Defense. For the Government of Japan, the competent authority shall be identified by the Government of Japan and notified by it to the Government of the United States of America through the diplomatic channel.

Article 6
Principles for Protecting CMI

The Parties shall ensure that:

(a) The recipient Party shall not release the CMI to any government, person, firm, institution, organization, or other entity of a third country without the prior written approval of the releasing Party;

(b) The recipient Party, in accordance with its
national laws and regulations, shall take appropriate measures to provide to the CMI a degree of protection substantially equivalent to that afforded by the releasing Party;

(c) The recipient Party shall not use the CMI for any other purpose than that for which it was provided, without the prior written approval of the releasing Party;

(d) The recipient Party shall observe intellectual property rights such as patents, copyrights, or trade secrets applicable to CMI, in accordance with its national laws and regulations;

(e) Each governmental facility that handles CMI shall maintain a registry of individuals with personnel security clearances and who are authorized to have access to such information; and

(f) Procedures for identification, location, inventory, and control of CMI shall be established by each Party to manage the dissemination of and access to CMI.

Article 7
Personnel Access to CMI

(a) No government official shall be entitled to access to CMI solely by virtue of rank, appointment, or a personnel security clearance.

(b) Access to CMI shall be granted only to those government officials whose official duties require such access and who have been granted a personnel security clearance in accordance with the national laws and regulations of the recipient Party.

(c) The Parties shall ensure that the determination on the granting to a government official of a personnel security clearance is consistent with the interests of national security and based upon all available information indicating whether the government official is trustworthy and reliable in the handling of CMI.

(d) Appropriate procedures shall be implemented by the Parties to ensure that the criteria referred to in the preceding paragraph have been met, in accordance with the national laws and regulations of each Party, with respect to any government official to be granted access to CMI.
Before a representative of one Party releases CMI to a representative of the other Party, the recipient Party shall provide to the releasing Party an assurance that: the representative possesses the necessary level of personnel security clearance; the representative requires access for official purposes; and that the recipient Party, in accordance with its national laws and regulations, shall take appropriate measures to provide to the CMI a degree of protection substantially equivalent to that afforded by the releasing Party.

Article 8
Visit Procedures

Authorizations for visits by representatives of one Party to facilities of the other Party where access to CMI is required shall be limited to those necessary for official purposes. Authorization to visit a facility that is located in the territory of the country of one Party shall be granted only by the Party. The visited Party shall be responsible for advising the facility of the proposed visit, the topic, the scope, and highest level of CMI that may be furnished to the visitor. Requests for visits by representatives of the Parties shall be submitted through the appropriate offices of the Embassy of the United States of America in Tokyo or United States Forces Japan Headquarters in the case of United States visitors, and through the Embassy of Japan in Washington, D.C. in the case of Japanese visitors.

Article 9
Transmission

CMI shall be transmitted between the Parties through Government-to-Government channels. Upon such transfer, the Recipient Party shall assume responsibility for custody, control, and security of the CMI.

Article 10
Security of Facilities

Each Party shall be responsible for the security of all governmental facilities where CMI of the other Party is kept and shall assure that for each such facility qualified government officials are appointed who shall have the responsibility and authority for the control and protection of CMI subject to this Agreement.

Article 11
Storage
The Parties shall store CMI in a manner that ensures access only by those individuals who have been authorized access pursuant to Articles 7 and 16.

Article 12
Security Requirements during Transmission

The minimum requirements for the security of CMI during transmission shall be as follows:

(a) Classified documents and media

(i) Documents and media containing CMI shall be transmitted in double, sealed envelopes with the innermost envelope bearing only the classification of the documents or media and the organizational address of the intended recipient and the outer envelope bearing the organizational address of the recipient, the organizational address of the sender, and the registry number, if applicable.

(ii) No indication of the classification of the enclosed documents or media shall be made on the outer envelope. The sealed envelope shall then be transmitted according to the prescribed regulations and procedures of the releasing Party.

(iii) Receipts shall be prepared for packages containing classified documents or media that are transmitted between the Parties and a receipt for the enclosed documents or media shall be signed by the final recipient and returned to the sender.

(b) Classified equipment

(i) Classified equipment shall be transported in sealed, covered vehicles or be securely packaged or protected in order to prevent identification of its details, and kept under continuous control to prevent access by unauthorized persons.

(ii) Classified equipment that must be stored temporarily awaiting shipment shall be placed in a storage area that provides protection commensurate with the level of classification of the equipment. Only authorized personnel shall have access to the storage area.
(iii) Receipts shall be obtained on every occasion when classified equipment changes hands en route.

(iv) Receipts shall be signed by the final recipient and returned to the sender.

(c) Electronic transmissions

CMI transmitted by electronic means shall be protected during transmission using encryption appropriate for that level of classified information. Information systems processing, storing, or conveying CMI shall receive security accreditation by the appropriate authority of the Party employing the system.

Article 13
Destruction

(a) The Parties shall destroy classified documents and media by burning, shredding, pulping, or other means preventing reconstruction in whole or in part of the CMI.

(b) The Parties shall destroy classified equipment beyond recognition or modify it so as to preclude reconstruction in whole or in part of the CMI.

Article 14
Reproduction

When the Parties reproduce classified documents or media, they shall also reproduce all original security markings thereon or mark on each copy. The Parties shall place such reproduced classified documents or media under the same controls as the original classified documents or media. The Parties shall limit the number of copies to that required for official purposes.

Article 15
Translations

The Parties shall ensure that all translations of CMI are done by individuals with personnel security clearances pursuant to Articles 7 and 16. The Parties shall keep the number of copies to a minimum and control the distribution. Such translations shall bear appropriate security classification markings and a suitable notation in the language into which it is translated indicating that the document or media contains CMI of the releasing Party.
Article 16
Release of CMI to Contractors

Prior to the release to a contractor (including a subcontractor, whenever the term is used herein) of any CMI received from the other Party, the recipient Party shall take appropriate measures, in accordance with its national laws and regulations, to ensure that:

(a) no individual is entitled to access to CMI solely by virtue of rank, appointment, or a personnel security clearance;

(b) the contractor and the contractor's facilities have the capability to protect CMI;

(c) all individuals whose official duties require access to CMI have personnel security clearances;

(d) a personnel security clearance is determined in the same manner as provided for in Article 7;

(e) appropriate procedures are implemented to provide assurance that the criteria referred to in Article 7(c) have been met with respect to any individual granted access to CMI;

(f) all individuals having access to CMI are informed of their responsibilities to protect the information;

(g) initial and periodic security inspections are carried out by the recipient Party at each contractor facility where the releasing Party's CMI is stored or accessed to ensure that it is protected as required in this Agreement;

(h) access to CMI is limited to those persons whose official duties require such access;

(i) a registry of individuals with personnel security clearances and who are authorized to have access to such information is maintained at each facility;

(j) qualified individuals are appointed who shall have the responsibility and authority for the control and protection of CMI;

(k) CMI is stored in the same manner as provided for in Article 11;

(l) CMI is transmitted in the same manner as provided
for in Articles 9 and 12;

(m) classified documents and classified equipment are destroyed in the same manner as provided for in Article 13;

(n) classified documents are reproduced and placed under control in the same manner as provided for in Article 14; and

(o) translation of CMI is done and copies are treated in the same manner as provided for in Article 15.

Article 17
Loss or Compromise

The releasing Party shall be informed immediately of all losses or compromises as well as possible losses or compromises of its CMI and the recipient Party shall initiate an investigation to determine the circumstances. The results of the investigation and information regarding measures taken to prevent recurrence shall be forwarded to the releasing Party by the recipient Party.

Article 18
Visits by Security Representatives

Implementation of the foregoing security requirements can be advanced through reciprocal visits by security representatives of the Parties. Accordingly, security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss security procedures and observe their implementation in the interest of achieving reasonable comparability of their respective security systems on mutually agreed venues and in a mutually satisfactory manner. Each Party shall assist the security representatives in determining whether CMI provided by the other Party is being adequately protected.

Article 19
Entry into Force, Amendment, Duration and Termination

(a) This Agreement shall enter into force on the date of signature.

(b) Amendments to the present Agreement shall be entered into by mutual written consent of the Parties and shall enter into force on the date of the signature thereof.

(c) This Agreement shall remain in force for a period of one year and shall be automatically extended
annually thereafter unless either Party notifies the other in writing through the diplomatic channel ninety days in advance of its intention to terminate the Agreement.

(d) Notwithstanding the termination of this Agreement, all CMI provided pursuant to this Agreement shall continue to be protected in accordance with the provisions of this Agreement.

DONE at Tokyo on August 10, 2007, in duplicate, in the English and Japanese languages, both texts being equally authentic.

For the Government of the United States of America:

[Signature]

For the Government of Japan:

[Signature]
The Japanese national laws referred to in paragraph (b) of Article 1:

(a) Secret Protection Law to Implement the Mutual Defense Assistance Agreement and Other Related Agreements between Japan and the United States of America (Law No. 166, 1954)

(b) Self-Defense Forces Law (Law No. 165, 1954)

(c) Law on Special Measures concerning Criminal Cases to Implement the Agreement under Article VI of the Treaty of Mutual Cooperation and Security between Japan and the United States of America, regarding Facilities and Areas and the Status of United States Armed Forces in Japan (Law No. 138, 1952)

(d) National Public Service Law (Law No. 120, 1947)
秘密軍事情報の保護のための秘密保持の措置に関するアメリカ合衆国政府及び日本国政府（以下「両締結国政府」といいう。）は、前文

千九百六十年一月十九日にワシントンで署名されたアメリカ合衆国と日本国との間の相互協力及び安全保全条約に基づく両国間の安全保障体制が、共通の安全保障上の目標を達成するための基礎であることを確認し、

千九百五十四年三月八日に東京で署名されたアメリカ合衆国と日本国との間の相互防衛援助協定及び同協定に基づく取極が、防衛関連情報の相互の交換を規定してきたことを認識し、

二千五年十月二十九日の安全保障関連情報の保護を確保するために必要な追加的措置をとる約束を表明したことを想起し、

次のとおり協定した。
一方の締約国政府は、この協定の下での秘密軍事情報の保護に影響を及ぼす自国の国内法令のいかなる変更についても、他方の締約国政府に対し通報する。この場合には、両締約国政府は、第十九条(b)に規定する情報を提供する締約国政府の書面により別段の承認を行わない限り、引き続きこの協定の規定に従って保護される。
第五条
補足実施取極

この協定に基づき補足実施取極は、両締約国政府の権限のある当局により行うことができる。アメリカ合衆国政府については、権限のある当局は、日本国政府により権限のある当局は、日本の政府において、権限のある当局は、日本の政府において、権限のある当局は、日本の政府により秘められたものとする。

第六条
締約国政府は、次の場合を保護されるための原則

(a) 秘密軍事情報を受領する締約国政府は、当該情報の提供する締約国政府の事前の書面による承認を得ることなく、第三国政府、個人、企業、機関、組織又は他の団体に対し、当該情報を提供しないこと。
秘密軍事情報を受領する締約国政府は、当該情報が提供された目的以外の目的のために、当該情報を使用しないこと。（c）

団又は企業秘密のような知的財産権を遵守すること。（d）

秘密軍事情報を受領する締約国政府は、自国の国内法令に従って、当該情報を使用しないこと。（e）

各締約国政府は、秘密軍事情報の配布及び当該情報へのアクセスを許可されていない個人の登録簿を保持すること。（f）

别、所在地、目録及び管理の手続を設定すること。（g）

秘密軍事情報へのアクセスは、政府職員であって、職務上当該アクセスを必要とし、かつ、当該情報の識を受領する締約国政府の国内法令に従って秘密軍事情報取扱資格を付与されたものに対してのみ認めら
両締約国政府は、政府職員が秘密軍事情報を取扱うに当たり、その入手可能な情報に基づき行われることを確保する。

一方の締約国政府の代表者が、他方の締約国政府の代表者に対し、秘密軍事情報を提供する際には、次のような事項についての保証を与えること。

(i) 当該情報をおける締約国政府により与えられている保護と実質的に同等の保護を与えるためには、適当な措置をとること。

(ii) 当該情報をおける締約国政府の国内法令に従って、当該情報について、当該情報をおける締約国政府によって、当該情報をおける締約国政府は、自国の国内法令に従って、当該情報について、当該情報をおける締約国政府が、必要な水準の秘密軍事情報取扱資格を有すること。
一方の締約国政府の代表者が、他方の締約国政府の施設であって、秘密軍事情報へのアクセスを必要とするものを訪問するための許可は、公用的目的のために必要なものに限定される。一方の締約国政府は、訪問先の施設に対し、訪問案、主题、範囲及び訪問者に対し提供するべき、情報の管理及び秘密保持の責任を有する。両締約国政府の代表者による訪問のための申請は、合衆国の訪問者の場合に於てはワシントンの日本大使館を通じて、提出される。
秘密軍事情報を提供する締約国政府の定められた規則及び手続きに従って送付される。秘密指定された装備

(i) 秘密指定された装備は、その管理者が識別されることを防止するために、封印され、被覆された保管箱に保管され、発送される。

(ii) 発送を待つ間、一時的に保管されなければならず、管理の下に置かれる。水準に応じた保護を与える保管区域に置かれる。許可された職員のみが、当該保管区域にアクセスするものとする。

(iii) 送付される間に、秘密指定された装備の管理者が変わる場合には、受領証は、その都度取得される。
(iv) 受領証は、最終の受領者により署名され、発送者に返還される。
(c) 電子的送付
号を使用することにより送付される秘密軍事情報は、送付される間、当該秘密情報の原文を照らし適当な暗号を使用する締約国政府の適当な当局により、秘密保持についての認定を受ける。
第十三条
(b) 両締約国政府は、秘密情報の全部又は一部の復元を防止するために、秘密指定された装備を見分ける方法により、秘密指定された装備を変更する。
第十四条
(c) 両締約国政府が秘密指定された文書又は媒体を複製するときは、これらに付されているすべての秘密指定を、このような複製された秘密指定を、
第十五条 翻訳
両締約国政府は、秘密軍事情報のすべての翻訳が、第七条及び次条の規定に従って秘密軍事情報取扱資格の有する個人により行われることを確保する。両締約国政府は、複製物の数を最小限にとどめるために、その配布を管理する。当該翻訳には、適当な秘密指定を付すものとし、かつ、文書又は媒体が当該文書又は媒体を提供する締約国政府の秘密軍事情報を含むことを示す適当な注釈を翻訳された後の言語により付すものとする。

第十六条 契約企業への秘密軍事情報の提供
秘密軍事情報を受領する締約国政府は、当該情報を提供する締約国政府から受領する当該情報が契約企業（下請契約企業を含む。以下同じ。）に対し提供する前に、自国の国内法令に従って、次の事項を確保することに適当な措置をとる。

(a) いかなる個人も、階級、地位又は秘密軍事情報取扱資格の有する人により、秘密軍事情報へのアクセスを認
契約企業及び契約企業の施設が、秘密軍事情報を保護する能力を有すること。

職務上秘密軍事情報へのアクセスを必要とするすべての個人が、秘密軍事情報取扱資格を有すること。

秘密軍事情報取扱資格が、第7条に規定する方法と同様の方法により決定されること。

職務上秘密軍事情報へのアクセスを有するすべての個人に関して、第7条(c)に規定する基準が満たされていることを保証するために、適当な手続が実施されること。

秘密軍事情報を受領する締約国政府は、当該情報を提供する締約国政府の当該情報がこの規定において、最初の及び定期的な保安検査を実施すること。

秘密軍事情報へのアクセスが、職務上当該アクセスを必要とする個人に限定されること。
秘密軍事情報取扱資格を有し、かつ、当該情報にアクセスすることを許可されている個人の登録簿が、各施設において保持されること。

秘密軍事情報の管理及び保護の責任及び権限を有する適格な個人が、指名されること。

秘密軍事情報が、第九条及び第十二条に規定する方法と同様の方法により保管されること。

秘密軍事情報が、第十一条に規定する方法と同様の方法により保管されること。

秘密指定された文書及び秘密指定された装備が、第十四条に規定する方法と同様の方法により破壊されること。

秘密軍事情報の翻訳が、前条に規定する方法と同様の方法により送付されること。

秘密軍事情報の翻訳が、前条に規定する方法と同様の方法により送付されること。

秘密指定された文書が、第十四条に規定する方法と同様の方法により破壊されること。

秘密軍事情報を提供する締約国政府は、当該情報のあらゆる紛失又は漏せつ及び紛失又は漏せつのあらゆ

第十七条
紛失又は漏せつ

により取り扱われること。

第十七条
紛失又は漏せつ
可能

性にについて直接に通知され、当該情報を受領する締約国政府は、当該情報を提供する締約国政府に対し、当該調査の結果及び再発を防止するためにとられる措置に関する情報を送付する。

前記の秘密保持に関する義務の履行は、締約国政府の秘密保持に係る代表者による訪問

進行することができる。このため、一方の締約国政府の秘密保持に係る代表者は、それぞれの秘密保持制度が合理的な程度に同等のものとなることを達成するために、秘密保持の手続きについて議論し、及びその実施を視察することができる。この目的に際して、相互に合意する場所において、及び相互に満足する方法により、事前の協議の後、他方の締約国政府を訪問することが許可される。一方の締約国政府は、他方の締約国政府により提供される秘密軍事情報が適切に保護されているか否かについて、秘密保持に係る代表者に決定することに当たる。
页码16

内容：

①

②

③

④

⑤