Section 3. Efforts to Prevent the Leakage of Information

Leakage of some information handled by the Ministry of Defense could have serious impact on the defense of Japan. Protection of such classified information is the essential foundation to fulfill defense of our country and maintain security of our country. Accordingly, the Ministry of Defense defines three types of classified information and stipulates procedures for designation and handling, such as communication, storage and disposal for each information, in order to prevent unauthorized personnel from inappropriately accessing the information in an effort to protect it. The three types of classified information are: “Special Defense Secret,” which is information concerning materials, equipment, etc. provided by the United States based on the Mutual Defense Assistance Agreement between Japan and the United States of America; “Defense Secret,” which is designated by the Minister of Defense as information concerning SDF operations, build-up of defense capabilities, etc. that must be kept secret for national defense; and the so-called “Ministry of Defense Secret,” which is classified information, other than those listed above, related to administrative work of the Ministry of Defense.

The following incidents where classified information was leaked have taken place at the Ministry of Defense and the Self-Defense Forces, as explained below.

This section explains the points of issue arising from these incidents and measures taken based on them.

1. Recent Incidents

1. Incident of Information Leakage via the Internet

A series of information leakage via the Internet occurred at the Ministry of Defense and the Self-Defense Forces. In February 2006, an incident of leakage of classified information on the destroyer *Asayuki* from a privately-owned personal computer through file-sharing software came to light.

The fact that the Ministry of Defense’s information security systems and awareness of personnel have not kept abreast of recent rapid IT innovation is in the background of this incident.

2. Incident of Leakage of Special Defense Secret Concerning the Aegis System

In January 2007 it was discovered that a crew member of the destroyer *Shirane* had saved information that was thought to be classified on an external hard disk at the crew member’s home, and as a result of investigations, in December 2007, an MSDF officer was arrested on suspicion of leaking Special Defense Secrets concerning the Aegis system, and four other MSDF officers were sent to the prosecutor.

The following problems are considered to have contributed to this incident: (1) lack of awareness concerning information security, including violation of rules and the fact that they easily copied the classified documents; (2) an incomplete system for protecting classified information, including the implementation of education involving classified information without approval; (3) incomplete management of personal computers (this incident emerged prior to the implementation of drastic measures to prevent a recurrence of a leakage of information via the Internet, as described above); and (4) insufficient monitoring and surveillance by managers and persons responsible for the protection of classified information.

As a result of investigations into this incident, although it was not confirmed that Special Defense Secrets had been leaked outside the SDF, there is a possibility that external leakage could have occurred in consideration of the fact that confidential information about the Aegis system was leaked to numerous SDF personnel. This was a very serious problem involving information security. This incident could have resulted in significant distrust among the public concerning the information security of the MSDF and indeed the SDF as a whole, and has also impacted the Japan-U.S. Security Arrangements and relations with other countries. Furthermore, it has had a severe impact on the morale of SDF personnel.
The Ministry of Defense has examined and investigated the facts of this incident and in March 2008, the result was reported to the public.

2. Efforts at the Ministry of Defense

In February 2006, in response to the incident of information leakage via the Internet, the Ministry of Defense took a number of emergency measures, including removal of file-sharing software installed on privately-owned personal computers which had been used for work; removal of classified information and unnecessary data relating to work; and total prohibition of the use of privately-owned personal computers to handle classified information.

In addition to these emergency measures, in February 2006, the Commission on Drastic Measures to Prevent Recurrence of Computer Related Classified Information Leakages, headed by the then Parliamentary Secretary for Defense, was established. The Commission discussed specific drastic measures to prevent recurrence and released them in April 2006. After that, in April 2006, the Committee to Implement Measures for the Prevention of the Recurrence of Computer Related Classified Information Leakages, headed by the then Parliamentary Secretary for Defense was established, and it has endeavored to take specific measures.

Under the circumstances, the incident of the leakage of Special Defense Secrets concerning the Aegis system came to light. In response to it, the Committee to Implement Measures for the Prevention of the Recurrence of Computer Related Classified Information Leakages was abolished, and the Council for Prevention of Information Leakage, headed by the Minister of Defense, was newly established in April 2007. This Council is engaged in consideration and implementation of measures, based on an awareness that the importance of information management and drastic measures to prevent leakages have not sufficiently permeated through the terminal members of the Defense Ministry and the SDF.

The major measures implemented to date by the Ministry of Defense and the SDF concerning prevention of information leakage are shown in Fig. IV-3-1.

The Ministry of Defense and the SDF would like to continue such efforts based on the report by the Council for Reforming the Ministry of Defense in July 2008.
New Establishment of the “Self-Defense Forces Intelligence Security Unit” (Provisional Name)

The Intelligence Security Unit is a unit established within the Ground, Maritime and Air Self-Defense Forces to collect and sort out information necessary for implementing information security works at units.

It has become extremely important to strengthen the posture for information security in the Ministry of Defense in response to a series of incidents of information leakage. Based on the recognition that it has become increasingly necessary for the Ministry of Defense to protect sensitive information gained by the Self-Defense Forces from intelligence activities by foreign countries, in the budget for FY 2008, the intelligence security units placed in the Ground, Maritime and Air Self-Defense Forces are to be integrated into a newly established unit called the SDF Intelligence Security Unit (provisional name), and a necessary increase in the staff is being planned.

Through this reorganization, it will be possible to conduct efficient gathering, collection, analysis and sharing of information on intelligence activities against the SDF, thereby strengthening the information security posture for counter-intelligence.

* Planned to be established during FY 2008 aiming at developing operation policies and others of the SDF Intelligence Security Unit (provisional name) and the gathering and sharing of counter-intelligence-related information.
**Fig. IV-3-1 Principal Measures for the Prevention of Information Leakage**

### Measures involving people

<table>
<thead>
<tr>
<th>Necessary measures for security of classified information</th>
<th>Measures taken by the Ministry of Defense</th>
</tr>
</thead>
</table>
| ☑ Limitation of those with access to classified information | ☑ The manager will designate “suitable persons” as persons who handle classified information (Decision made based on consideration of personal history and specific individual details such as daily work attitude)  
☑ Minimize appointments under the “principles of need to know”* |
| ☑ Recognition of the importance of information management | ☑ Submit “contracts” in order to raise awareness of the significant responsibility associated with the protection of classified information  
☑ Clarify the responsibility of managers and others handling classified information  
☑ Implementation of private training for all unit members involved in Information Leakage Prevention  
☑ Dispatch to the unit a special activity team headed by an internal bureau executive personnel |
| ☑ Familiarization of those handling classified information with specific rules | ☑ Periodically implement education on information protection to all staff according to grades and information  
☑ Prepare and distribute a compilation of examples, and confirm the degree of comprehension, as well as establish monthly information security  
☑ Organize and unify dispersed regulations for protection of classified information, and establish a coherent structure |
| ☑ Reinforcement of deterrent against leakage of classified information | ☑ After thorough scrutiny of information concerning “MOD Secret (classified • top secret),” shift them to “Defense Secret” guaranteed by strict penalty (Strengthening of disciplinary action by establishment of Classified Information of Defense System by revision to the Self-Defense Forces Law in 2001 and implemented in 2002)  
☑ Define the disciplinary action standards in regards to information leakage  
☑ Utilization of the Whistleblowing Act  
☑ Inspection by the Inspector General’s Office of Legal Compliance |

* : Principle of “sharing information only with those who require it, and not sharing information with those who do not require it.”

☐ : Measures following the establishment of “Fundamental Measures for the Prevention of the Recurrence of Computer Related Classified Information Leakages” in April 2006.

☑ : Implemented since April 2007 following the incident in which MSDF unit informally removed classified information.

### Measures involving Classified Documents

<table>
<thead>
<tr>
<th>Necessary measures for security of classified information</th>
<th>Measures taken by the Ministry of Defense</th>
</tr>
</thead>
</table>
| ☑ Prohibition of the removal of classified documents | ☑ The person in charge in each division will unitarily conduct the storage of classified documents  
☑ Classified documents will be logged in a book, and then kept in a safe deposit, etc. with a three-level dial lock  
☑ Installation of a security and alarm system at some entrances of government office buildings that detect and warn against taking out of classified documents |
| ☑ Leakage prevention when mailing to external sources | ☑ In order to send or lend classified documents to external persons, manager approval is necessary and those actions must be recorded in the register  
☑ Use of telephones and faxes that conceal contents by encryption for transmission of classified information |
| ☑ Restricted access to facilities handling classified information | ☑ Prohibit access to most facilities handling classified information. Access to such places, managed by IC card, password or verification |
| ☑ Reduction of classified documents | ☑ Prevent an excess of classification designs as well as reduce classified documents by taking measures to make stricter designations of classified information |

☐ : Measures following the establishment of “Fundamental Measures for the Prevention of the Recurrence of Computer Related Classified Information Leakages” in April 2006.
### Measures involving electronic data

<table>
<thead>
<tr>
<th>Necessary measures for security of classified information</th>
<th>Measures taken by the Ministry of Defense</th>
</tr>
</thead>
</table>
| ☑ Prohibition of the removal of administrative data outside of the workplace without consent | ☑ Removal of private computers from the workplace  
- Emergency supply of computers owned by the ministry (around 56,000 computers, around ¥4 billion)  
- Prohibit use of personal computers inside workplace  
- Prohibit use of privately-owned portable memory devices on official computers  
- Prevent the unauthorized taking out of data  
- Execute inspections without notice of personal belongings during work hours and upon arriving/departing work  
- Prevent the removal of work-related data by installing file encryption software  
- Clearly mark and strictly manage official portable memory devices  
- Verification of adherence to the measures concerning information guarantee, such as inspections of the official portable memory devices management book (Periodic investigation once a year, special investigation once a year, dispatch of the special investigation team if a third person is secured.) |
| ☑ Prohibition of work-related data handling on computers at home, etc. | ☑ Erase all unnecessary classified data as well as file-sharing software from personal computers once used for work purposes  
- Educate relevant persons on the dangers of information leakage by file-sharing software and promote removal of such software  
- Following the submission of a written oath that states the handling of no administrative data on personal computers and such, obtain consent from the individual to check whether or not private computers at home contain administrative work-related data  
- In regards to the “check” as mentioned above, make one round of all staff members by the end of July 2007, and toughen penalty thereafter |
| ☑ Reinforcement of information management system | ☑ Regarding the manager assistant, appointment is made by considering knowledge of the treatment of computers, etc., and not just simply appointment |

◊ : Measures following the establishment of “Fundamental Measures to the Prevention of the Recurrence of Computer Related Classified Information Leakages” in April 2006.  
☐ : Measures following the establishment of “Fundamental Measures for the Prevention of the Recurrence of Computer Related Classified Information Leakages” in April 2006.  
☐ : Implemented since April 2007 following the incident in which MSDF unit informally removed classified information.