REPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat Général de la Défense Nationale

N° 730/ SCSSI

Issy-les-Moulineaux, le 13 janvier 1997

GUIDE INTERMINISTERIEL

SUR LES

SYSTEMES D'INFORMATION ET

APPLICATIONS SENSIBLES

SERVICE CENTRAL DE LA SECURITE DES SYSTEMES D'INFORMATION

MISE EN APPLICATION

Elaboré par la sous-commission n°4 de la commission interministérielle pour la sécurité des systèmes d'information et par le Service central de la sécurité des systèmes d'information, ce guide propose la démarche à suivre dans l'établissement et la mise à jour des répertoires des systèmes d'information et applications sensibles des départements ministériels.

Sa mise en application prend effet à compter du 13 janvier 1997.

Le Chef du Service central
de la sécurité des systèmes d'information

S O M M A I R E

INTRODUCTION

La défense a pour objet d'assurer en tout temps, en toutes circonstances et contre toutes les formes d'agression, la sécurité et l'intégrité du territoire, ainsi que la vie de la population (Ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense, article 1er).

Chaque ministre est responsable de la préparation et de l'exécution des mesures de défense incombant au département dont il a la charge (article 15 de l'ordonnance précitée). En outre, le ministre de l'intérieur [1] est investi d'une responsabilité générale. Il est chargé en effet, de préparer en permanence et de mettre en oeuvre la défense civile. "Il est responsable à ce titre de l'ordre public, de la protection matérielle et morale des personnes et de la sauvegarde des installations et ressources d'intérêt général" (article 17 de l'ordonnance précitée).

La défense nécessite notamment la mise en oeuvre de systèmes d'information et d'applications sur lesquels s'exerce une menace permanente.

Afin d'assurer la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir, en situation normale comme en situation de crise, ces systèmes d'information et applications nécessitent des mesures propres à en garantir la sécurité.

La protection de ces systèmes d'information et applications passe par leur recensement préalable.

A cet effet, il est recommandé à chaque haut fonctionnaire de défense de veiller à l'établissement et à la mise à jour des répertoires des systèmes d'information et applications sensibles de son département ministériel.

En vue d'aider les hauts fonctionnaires de défense à fixer les orientations pour l'établissement de ces répertoires, le présent guide a pour objet de :

- définir les systèmes d'information et applications sensibles,
- fournir les indications permettant de les identifier et de les recenser,
- proposer une méthode pour leur classement et leur inscription dans les répertoires, ainsi que les conseils utiles pour l'établissement et la tenue à jour des répertoires.

[1] Dans les départements et territoires d'outre-mer, cette responsabilité est assumée par le ministre des DOM-TOM (article 1er du décret n° 64-11 du 3 janvier 1964 modifié relatif à l'organisation des responsabilités territoriales de défense dans les départements et territoires d'outre-mer).

I - DOMAINE D'APPLICATION

Le présent guide concerne :

1°) les systèmes d'information et applications sensibles des départements ministériels et des organismes sous tutelle, lorsque ces systèmes d'information et applications sensibles jouent un rôle dans la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir ;

2°) les systèmes d'information et applications sensibles exploités par d'autres personnes que l'Etat, qu'elles soient publiques ou privées, qu'il s'agisse de personnes morales ou physiques, lorsque ces systèmes d'information et applications sensibles jouent un rôle dans la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir.

II - DEFINITIONS ET CATEGORIES

2.1 - Systèmes d'information et applications

2.1.1 - Information

Le terme information désigne tout renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à un enregistrement, une communication ou un traitement. [2]

La notion d'information, de caractère immatériel, ne concerne que le contenu et non le support.

2.1.2 - Application

Le terme application désigne l'ensemble des moyens mis en oeuvre (logiciels, procédures correspondantes et contrôles) ou conçus pour atteindre un ensemble de buts précis. Dans un système informatique, les applications sont généralement supportées par des logiciels qui fournissent des fonctionnalités spécifiques aux utilisateurs de l'application.

2.1.3 - Système d'information

Est dénommé système d'information [2] tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.

Par souci de simplification, le terme "traiter" est généralement utilisé pour désigner l'ensemble de ces fonctions.

2.2 - Systèmes d'information et applications sensibles

2.2.1 - Information sensible

Une information sensible - au sens du présent guide - est une information dont la compromission, l'altération, le détournement ou la destruction, est de nature à nuire à la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir, en situation normale comme en situation de crise.

Une information sensible - au sens du présent guide - peut relever du secret de la défense nationale (Cf. article 413-9 du Code pénal) ou des intérêts fondamentaux de la nation (Cf. article 410-1 du Code pénal).

---

[2] Cf. IGI n° 900 SGDN du 20 juillet 1993.

2.2.2 - Application sensible

Une application sensible - au sens du présent guide - est une application qui traite une information sensible définie ci-dessus ou qui offre un service et dont la perte de confidentialité, d'intégrité ou de disponibilité porterait préjudice à la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir, en situation normale comme en situation de crise.

Cette définition peut s'appliquer à des applications développées spécifiquement pour les besoins de l'Etat, qu'elles soient ou non protégées pour elles-mêmes ou pour les informations traitées, ainsi qu'à des logiciels commerciaux utilisés pour traiter des informations sensibles.

Une application, initialement non sensible, devient sensible dès lors qu'elle est utilisée pour traiter des informations sensibles. Elle peut, selon le cas et en fonction des risques identifiés, soit être déclarée sensible pendant la durée de traitement des informations sensibles, soit être déclarée sensible de façon permanente.

2.2.3 - Système d'information sensible

Un système d'information sensible - au sens du présent guide - est un système d'information qui supporte une ou plusieurs applications sensibles définies ci-dessus, ou qui comporte une ou plusieurs informations sensibles définies ci-dessus, ou qui offre un service et dont la perte de sécurité porterait préjudice à la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir, en situation normale comme en situation de crise.

La sécurité d'un système d'information sensible - au sens du présent guide - relève soit de l'instruction générale interministérielle n 900 du 20 juillet 1993, soit de la recommandation n 901 DISSI du 2 mars 1994. Il est rappelé que la "sécurité d'un système d'information" est l'état de protection, face aux risques identifiés, qui résulte des mesures générales et particulières prises pour assurer la disponibilité du système, l'intégrité du système et de l'information, la confidentialité de l'information.

La définition d'un système d'information sensible ci-dessus peut s'appliquer à des systèmes d'information développés spécifiquement pour les besoins de l'Etat, qu'ils soient ou non protégés pour eux-mêmes ou pour les applications ou les informations traitées, ainsi qu'à des systèmes d'information commerciaux utilisés pour traiter des applications sensibles.

Un système d'information, initialement non sensible, devient sensible dès lors qu'il supporte des applications sensibles. Il peut, selon le cas et en fonction des risques identifiés, soit être déclaré sensible pendant la durée d'utilisation des applications sensibles, soit être déclaré sensible de façon permanente.

2.3 - Déclaration de systèmes et applications sensibles

Les systèmes d'information et les applications qui jouent un rôle dans la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir, en situation normale comme en situation de crise, sont déclarés "sensibles".

Peuvent également être déclarés "sensibles", certains systèmes d'information ou applications dont l'utilisation non contrôlée, ou non autorisée, ou dont une modification malveillante du fonctionnement, pourrait entraîner des conséquences dommageables pour la défense [(3)].

Cette déclaration entraîne pour ces systèmes d'information et applications :

- leur classement selon leur sensibilité, appréciée en fonction des conséquences vis à vis de la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir,
- leur inscription dans des répertoires établis à cet effet,
- la mise en oeuvre de mesures destinées à assurer leur sécurité et à garantir la continuité de leur fonctionnement normal.

Un système d'information, ou une application, peut être déclaré sensible à titre permanent ou à titre temporaire. Une déclaration à titre temporaire est envisageable lorsque les motifs de cette déclaration ne sont satisfaits que de façon temporaire, lorsque les périodes correspondantes sont parfaitement définies et contrôlables, et que les risques de perte de sécurité du système d'information, ou de l'application, entre ces périodes est nul ou totalement maîtrisé.

2.4 - Catégories de systèmes et applications sensibles

Les systèmes d'information sensibles et les applications sensibles sont classés en trois catégories définies comme suit :

- **1ère catégorie :** systèmes d'information et applications sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entrainer la **neutralisation** d'une fonction majeure dans le fonctionnement des services de l'Etat et l'exercice du pouvoir (fonction rendue totalement inexploitable pendant une durée inacceptable, avec des conséquences graves ou très graves);
- **2ème catégorie :** systèmes d'information et applications sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entrainer une **dégradation** du fonctionnement des services de l'Etat et de l'exercice du pouvoir (fonctionnement fortement et durablement perturbé, avec des conséquences importantes);
- **3ème catégorie :** systèmes d'information et applications sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entrainer une **gêne** dans le fonctionnement des services de l'Etat et l'exercice du pouvoir (fonctionnement faiblement perturbé, avec des conséquences limitées).

Le classement dans l'une ou l'autre des trois catégories ci-dessus est fonction de la nature, de la gravité et de l'étendue du danger potentiel, que présente l'atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes, applications et réseaux

(3) La défense est ici entendue au sens de l'ordonnance n°59-147 du 7 janvier 1959, dans tous ses aspects militaires et non militaires. Elle englobe donc les aspects liés à la protection des populations.

d'information sensibles, vis à vis de l'importance et du rôle de ceux-ci pour assurer la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir, en situation normale comme en situation de crise.

Le classement de certains systèmes d'information ou de certaines applications déclarés "sensibles" en raison du risque d'utilisation non contrôlée ou non autorisée, ou de modification malveillante du fonctionnement, susceptible d'entraîner des conséquences dommageables pour la défense [4], peut être fait selon les trois catégories ci-dessus. Les critères de classement sont à adapter en fonction des conséquences que l'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de ces systèmes d'information et applications, pourrait entraîner sur la sécurité.

[4] La défense est ici entendue au sens de l'ordonnance n°59-147 du 7 janvier 1959, dans tous ses aspects militaires et non militaires. Elle englobe donc les aspects liés à la protection des populations.

III - REPERTOIRES DES SYSTEMES ET APPLICATIONS SENSIBLES

3.1 - But des répertoires

Les répertoires des systèmes d'information sensibles et des applications sensibles ont pour but :

- de dresser l'inventaire des systèmes d'information sensibles et des applications sensibles devant bénéficier de mesures de protection;
- de fournir aux autorités responsables, aux différents échelons, une vue d'ensemble des systèmes d'information et applications sensibles de leur ressort;
- de servir de base à l'établissement, et le cas échéant à la mise en oeuvre, des plans de protection prenant en compte les différentes menaces jugées pertinentes vis à vis de ces systèmes et applications.

3.2 - Types de répertoires

3.2.1 - Répertoires ministériels

Les systèmes d'information sensibles et les applications sensibles de chaque département ministériel sont inscrits, par catégorie, dans un répertoire ministériel.

Chaque répertoire ministériel contient les renseignements essentiels sur les systèmes d'information et applications sensibles placés sous la responsabilité d'un ministère (pour l'ensemble de la métropole et des départements et territoires d'outre-mer).

Il appartient à chaque haut fonctionnaire de défense d'apprécier si les systèmes et applications sensibles de son département ministériel doivent, notamment pour des raisons pratiques ou de sécurité, faire l'objet d'un répertoire ministériel unique ou de plusieurs répertoires partiels dont l'ensemble constitue le répertoire ministériel complet. Ainsi, la confidentialité des renseignements portés dans les répertoires ministériels pourrait-elle être mieux garantie en constituant des répertoires partiels selon le principe de cloisonnement de l'information.

Cette centralisation ministérielle ne s'oppose pas aux éventuels échanges de renseignements entre services d'un ministère sur leurs systèmes d'informations et applications sensibles d'une part et entre départements ministériels sur leurs répertoires respectifs d'autre part. Dans le deuxième cas, il appartient à chaque ministre, sur avis du haut fonctionnaire de défense, de préciser les conditions de diffusion des renseignements relatifs aux systèmes d'informations et applications sensibles de son département ministériel.

La classification de ces répertoires est au minimum CONFIDENTIEL DÉFENSE.

Le processus d'établissement de ces répertoires fait l'objet des paragraphes 3.3 et suivants.

3.2.2 - Répertoire national

Une consolidation au niveau national peut, si nécessaire, être obtenue par le regroupement au sein d'un répertoire national de tout ou partie des renseignements portés dans les répertoires ministériels.

Le répertoire national des sytèmes d'information et des applications sensibles est établi et tenu à jour par le SCSSI, sur la base des propositions de chaque ministère concerné, et si nécessaire après arbitrage par le SGDN.

De même que les répertoires ministériels peuvent être cloisonnés pour des raisons de sécurité (cf. § 3.2.1 ci-dessus), le répertoire national peut aussi, selon le principe de cloisonnement, être constitué de plusieurs répertoires partiels dont l'ensemble constitue le répertoire national complet. Le choix, basé sur le juste équilibre entre le besoin de centralisation de renseignements nécessaires au niveau interministériel et les exigences de protection de ces renseignements, en incombe au SGDN après avis des ministères concernés.

Cette centralisation interministérielle ne s'oppose pas aux éventuels échanges de renseignements entre départements ministériels sur leurs répertoires respectifs.

Le répertoire national reçoit, en principe, la mention de classification SECRET DEFENSE.

3.3 - Etablissement des répertoires

L'établissement des répertoires repose sur le recensement des systèmes d'information et applications sensibles.

Le recensement est de la responsabilité de chaque HFD au sein de son département ministériel. Il donne à cet effet les consignes nécessaires, aux services de son département ministériel et, éventuellement, aux organismes ou entreprises placés sous sa tutelle.

Il fait en particulier établir, pour chaque système d'information et application sensible (au sens du présent guide) une fiche, dite "déclarative", permettant d'identifier de façon précise et complète chacun de ces systèmes et applications. Cette fiche met notamment en évidence les fonctions (majeures) assurées par le système ou l'application dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir, ainsi que les motifs de classement dans l'une des trois catégories définies au § 2.4 ci-avant.

La fiche déclarative d'un système d'information sensible ou d'une application sensible est établie par ou sous le contrôle de l'agent de sécurité des systèmes d'information (ASSI) chargé de la sécurité de ce système ou de cette application.

La fiche déclarative est adressée, au HFD, par l'autorité qualifiée responsable du système ou de l'application.

La fiche déclarative est classifiée, au minimum, CONFIDENTIEL DÉFENSE et n'est, en principe, pas diffusée à l'extérieur du département ministériel.

Le HFD, sur la base de la fiche déclarative, fait inscrire le système ou l'application dans le répertoire adéquat.

Lorsqu'un système ou une application sensible implique plusieurs département ministériels, une coordination entre les HFD concernés est établie, soit à l'initiative de l'un d'eux, soit sur demande d'un organisme interministériel.

Nota :

1- Des modèles de fiches déclaratives, des systèmes d'information sensibles d'une part et des applications sensibles d'autre part, sont donnés en annexes.

2- Les modifications devant être apportées à la déclaration d'un système d'information sensible ou d'une application sensible seront formulées selon les mêmes modèles.

3.4 - Contenu des fiches déclaratives

3.4.1 - Systèmes d'information sensibles

Pour chaque système d'information sensible (au sens du présent guide) la fiche déclarative comporte les renseignements suivants:

- l'identification du système d'information ;
- la ou les fonctions (majeures) qu'il assure dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir ;
- la catégorie de classement en système sensible ;
- le ou les motifs de classement dans cette catégorie (dont : menaces pertinentes, risques identifiés, conséquences vis à vis des fonctions assurées, ...) ;
- le ou les lieux d'implantation et de mise en oeuvre du système d'information, avec l'indication de leur classement éventuel en zones "réservées" ou "protégées" (au sens de l'IGI n 1300) ;
- l'identification de la fonction :
  - de l'autorité qualifiée, responsable de la déclaration,
  - de l'autorité d'exploitation,
  - de l'autorité d'homologation,
  - du responsable de la gestion de la configuration,
  - du responsable de la SSI ;
- le type d'informations traitées sur ce système ;
- le niveau (maximum) de protection des informations et applications sensibles (au sens du présent guide) qui y sont traitées ;
- la liste des applications sensibles mises en oeuvre sur le système d'information ;
- les classes d'utilisateurs du système d'information ;
- les types de supports d'information utilisés en entrée et sortie ;

- la description sommaire de l'architecture générale du système et l'indication des matériels et principaux logiciels constituant le système d'information ;
- la durée de la sensibilité du système (permanente ou temporaire); si la sensibilité est temporaire, les conditions à remplir pour lever la sensibilité du système sont précisées ;
- les références des documents de sécurité du système, y compris des plans d'urgence et de sauvegardes ;
- l'indication des moyens de sécurité en service sur le système ;
- l'indication des moyens de sécurité des communications (en cas de nécessité) ;
- la référence de la décision d'homologation du système d'information.

3.4.2 - Applications sensibles

Pour chaque application sensible (au sens du présent guide), la fiche déclarative comporte les renseignements suivants :

- l'identification de l'application ;
- la ou les fonctions (majeures) qu'elle assure dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir ;
- la catégorie de classement en application sensible ;
- le ou les motifs de classement dans cette catégorie (dont : menaces pertinentes, risques identifiés, conséquences vis à vis des fonctions assurées, ...) ;
- le ou les lieux d'exploitation et de détention des applications sensibles (y compris des sauvegardes des applications et des informations traitées) ;
- l'identification de la fonction :
  - de l'autorité qualifiée, responsable de la déclaration,
  - de l'autorité d'exploitation,
  - du responsable de la SSI ;
- le niveau de protection (éventuel) de l'application ;
- le niveau (maximum) de protection des informations sensibles traitées ;
- les procédures utilisées (avec indication des services ou organismes intervenants) pour le développement et la maintenance (corrective et évolutive) ;
- les conditions matérielles d'exploitation :
  - type de matériel, réseau éventuel, ...
  - protections (locaux, matériels, réseaux, ...)
  - procédures de mise en oeuvre et d'exploitation ;
- les autorités et services concernés par la mise en oeuvre de l'application et l'utilisation des résultats produits ;
- la durée de la sensibilité de l'application (permanente ou temporaire); si la sensibilité est temporaire, les conditions à remplir pour lever la sensibilité de l'application sont précisées ;
- l'identification du (ou des) système(s) sensible(s) utilisant cette application.

3.5 - Contenu des répertoires ministériels

3.5.1 - Systèmes d'information sensibles

Pour chaque système d'information sensible (au sens du présent guide) le répertoire comporte les renseignements suivants:

- l'identification du système d'information ;
- la ou les fonctions (majeures) qu'il assure dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir ;
- la catégorie de classement en système sensible ;
- le ou les motifs de classement dans cette catégorie (dont : menaces pertinentes, risques identifiés, conséquences vis à vis des fonctions assurées, ...) ;
- le ou les lieux d'implantation et de mise en oeuvre du système d'information, avec l'indication de leur classement éventuel en zones "réservées" ou "protégées" (au sens de l'IGI n° 1300) ;
- l'identification de la fonction de l'autorité qualifiée, responsable de la déclaration ;
- la liste des applications sensibles mises en oeuvre sur le système d'information.

3.5.2 - Applications sensibles

Pour chaque application sensible (au sens du présent guide), le répertoire comporte les renseignements suivants :

- l'identification de l'application ;
- la ou les fonctions (majeures) qu'elle assure dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir ;
- la catégorie de classement en application sensible ;
- le ou les motifs de classement dans cette catégorie (dont : menaces pertinentes, risques identifiés, conséquences vis à vis des fonctions assurées, ...) ;
- le ou les lieux d'exploitation et de détention des applications sensibles (y compris des sauvegardes des applications et des informations traitées) ;
- l'identification de la fonction de l'autorité qualifiée, responsable de la déclaration ;
- l'identification du (ou des) système(s) sensible(s) utilisant cette application.

3.6 - Constitution du répertoire national

Les éléments d'appréciation à prendre en compte pour l'inscription d'un système d'information ou d'une application sensible au répertoire national sont notamment :

- l'importance fonctionnelle du système ou de l'application au plan de la continuité de l'action gouvernementale ;
- son rôle dans l'organisation nationale (civile ou militaire) de la défense ;
- son rôle dans le cadre des structures essentielles de la vie nationale, en particulier en ce qui concerne les besoins essentiels de la population, sa sécurité, sa capacité de survie, etc...;
- son importance relative, par rapport à d'autres systèmes et applications susceptibles de rendre le même service ;
- sa vulnérabilité face aux menaces pertinentes et les difficultés (moyens, délais) à remédier aux atteintes à la sécurité du sytème ou de l'application.

Le répertoire national des systèmes d'information et applications sensibles, ainsi qu'indiqué au § 3.2.2, regroupe donc tout ou partie des renseignements relatifs aux systèmes d'information et applications sensibles choisis parmi ceux inscrits dans les répertoires ministériels, en respectant les éventuelles exigences de protection de ces renseignements.

Le SGDN donne aux départements ministériels les directives nécessaires à ce choix.

Chaque HFD propose au SGDN, en fonction des directives données par celui-ci, les extraits des répertoires de son département ministériel nécessaires à la constitution du répertoire national.

3.7 - Mise à jour des répertoires

Les modifications à apporter aux répertoires ministériels sont signalées au HFD concerné, sans délai, par les autorités qualifiées responsables des déclarations.

Les modifications à apporter au répertoire national sont signalées, annuellement, au SCSSI par les HFD.

La mise à jour des répertoires est effectuée, ponctuellement lors de modifications importances d'un système d'information sensible, annuellement par émission d'une nouvelle édition de chaque répertoire.

La mise à jour annuelle des répertoires ministériels est effectuée pour le 1er février.

La mise à jour annuelle du répertoire national est effectuée pour le 1er mai.

3.8 - Diffusion des répertoires

La diffusion de chaque répertoire ministériel, au sein du département ministériel qui l'a établi, est de la responsabilité du HFD de ce ministère. Les conditions de diffusion, à l'extérieur du département ministériel, sont établies par le HFD responsable, éventuellement en liaison avec l'échelon interministériel compétent.

La diffusion du répertoire national incombe au SCSSI. Elle est, en principe, limitée au SGDN et aux départements ministériels (pour les extraits les concernant). Les conditions de diffusion du répertoire national des systèmes d'information et applications sensibles sont définies par le SGDN.

ANNEXE 1

FICHE DECLARATIVE
SYSTEME D'INFORMATION SENSIBLE

<table>
<tr><td colspan="2">Déclaration : Initiale / Modificative
(1) [ ] [ ]</td><td>Organisme émetteur :</td></tr>
<tr><td rowspan="2">Références et dates (2)</td><td colspan="2">Présente déclaration :</td></tr>
<tr><td colspan="2">Déclaration précédente :</td></tr>
<tr><td colspan="3">Identification du système d'information (3) :</td></tr>
<tr><td colspan="3">Fonction(s) majeure(s) que le système assure dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir (4) :</td></tr>
<tr><td>Catégorie de classement (Cf. § 2.4 du guide)</td><td>1ère
[ ]</td><td>2ème
[ ]</td><td>3ème
[ ]</td></tr>
<tr><td colspan="3">Motifs de classement dans cette catégorie (5) :
(menaces pertinentes, risques identifiés, conséquences vis-à-vis des fonctions assurées, etc.)</td></tr>
<tr><td colspan="3">Lieux d'implantation et de mise en oeuvre du système (6) :
(indiquer leur classement éventuel en zones "réservées" ou "protégées" au sens de l'IGI n 1300)</td></tr>
<tr><td colspan="3">Applications sensibles mises en oeuvre sur le système (7) :
(joindre, si nécessaire, la liste en annexe à la présente fiche déclarative)</td></tr>
<tr><td colspan="3">Autorité qualifiée (responsable de la déclaration) Signature</td></tr>
</table>

Type(s) d'informations traitées sur le système :		
Niveau maximum de protection :		
Classe(s) d'utilisateurs du système : (joindre une annexe, si nécessaire)		
Type(s) de supports d'information utilisés en entrées/sortites :		
Description sommaire de l'architecture du système et indication des principaux matériels et logiciels le constituant : (joindre une annexe, si nécessaire)		
Références des documents de sécurité du système et indication des moyens de sécurité du système : (joindre une annexe, si nécessaire)		
Sensibilité du système ( ) :	Permanente **[ ]**	Temporaire **=>** Durée : **[ ]**
Conditions à remplir pour lever la sensibilité du système ( ) :		
Référence de la décision d'homologation du système d'information :		
Autorité d'homologation :		**Autorité d'exploitation** :
Responsable gestion de configuration:		**Agent de sécurité du système** :

ANNEXE 2

FICHE DECLARATIVE
APPLICATION SENSIBLE

Déclaration : Initiale / Modificative (1) **[ ] [ ]**		**Organisme émetteur** :
Références et dates (2)	**Présente déclaration** :	
	Déclaration précédente :	

Identification de l'application (3) :

Fonction(s) majeure(s) que l'application assure dans le fonctionnement des services de l'Etat ou de l'exercice du pouvoir (4) :

Catégorie de classement (Cf. § 2.4 du guide)	**1ère** [ ]	**2ème** [ ]	**3ème** [ ]

Motifs de classement dans cette catégorie (5) :
(menaces pertinentes, risques identifiés, conséquences vis-à-vis des fonctions assurées, etc.)

Lieux d'exploitation et de détention de l'application (6) :
[y compris des sauvegardes de l'application et des informations traitées]

(indiquer leur classement éventuel en zones "réservées" ou "protégées" au sens de l'IGI n° 1300)

Système(s) d'information sensible(s) supportant l'application (7) :
et référence(s) de la (des) fiche(s) déclarative(s) correspondante(s)

(joindre, si nécessaire, la liste en annexe à la présente fiche déclarative)

Autorité qualifiée (responsable de la déclaration) Signature

Type(s) d'informations traitées par l'application :		
Niveau maximum de protection ( ) :	de l'application :	des informations traitées :
Procédures utilisées pour le développement et la maintenance, avec indication des services et organismes intervenants ( ) : (joindre une annexe, si nécessaire)		
Conditions matérielles d'exploitation		
Type de matériels, réseau(x) éventuel(s) (joindre une annexe, si nécessaire)		
Protections (locaux, matériels, réseaux, …) (joindre une annexe, si nécessaire)		
Procédures de mises en oeuvre et d'exploitation : (joindre une annexe, si nécessaire)		
Sensibilité de l'application ( ) :	Permanente **[ ]**	Temporaire **=>** Durée : **[ ]**
Conditions à remplir pour lever la sensibilité de l'application ( ) :		
Autorités et services concernés par la mise en oeuvre de l'application et l'utilisation des résultats produits :		
Autorité d'exploitation :	**Agent de sécurité** :	