

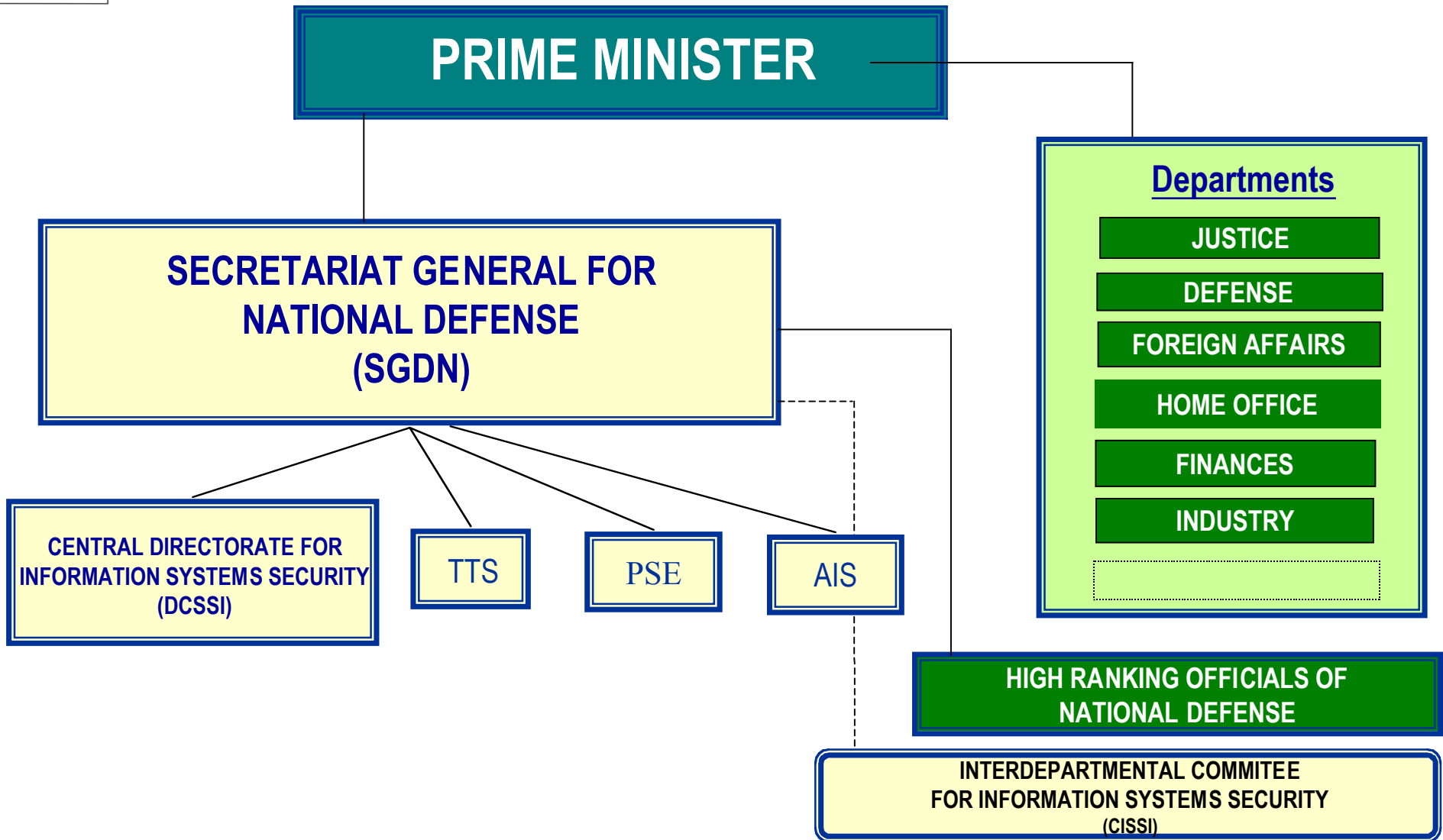


Secrétariat général de la défense nationale
(Secretariat General for National Defense)

Direction centrale de la sécurité des systèmes d'information
(Central Directorate for Information Systems Security)

CERTA

ISS organisation in France



Missions of the DCSSI

- ✓ **To contribute to interdepartmental definition** and expression of governmental policy as regards Information Security (IS)
- ✓ **To provide a regulatory function** of national authority for IS
- ✓ **To assist public services** in IS (councils, audits, CERTA, ...)
- ✓ **To develop scientific and technical expertise** in the field of the IS, for the benefit of the administration and public services
- ✓ **To run training courses** and increase awareness in IS

Organisation of the DCSSI



French CSIRTs

- Three CSIRTs in France:
 - **CERT-RENATER**, part of GIP RENATER (Academic Network)
(Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche)
 - **CERT-IST** (Industrie Services et Tertiaire) created by the end of 1998 (four partners: ALCATEL, le CNES, ELF and France Télécom)
 - **CERTA**
(Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques)

CERTA Declaration

- Decision of “Comité Interministériel pour la Société de l’Information” (CISI) on 19 January 1999:

“To strengthen State networks against attacks

In order to strengthen and to co-ordinate the struggle against intrusion into governmental computer systems, the government decide to create an assistance and warning team, whose missions are to watch and to answer issue related to computer attacks”

CERTA History

- ✓ Created by the end of 1999



FIRST member since 12 September 2000



Trusted Introducer (level 0) since 21 September 2000



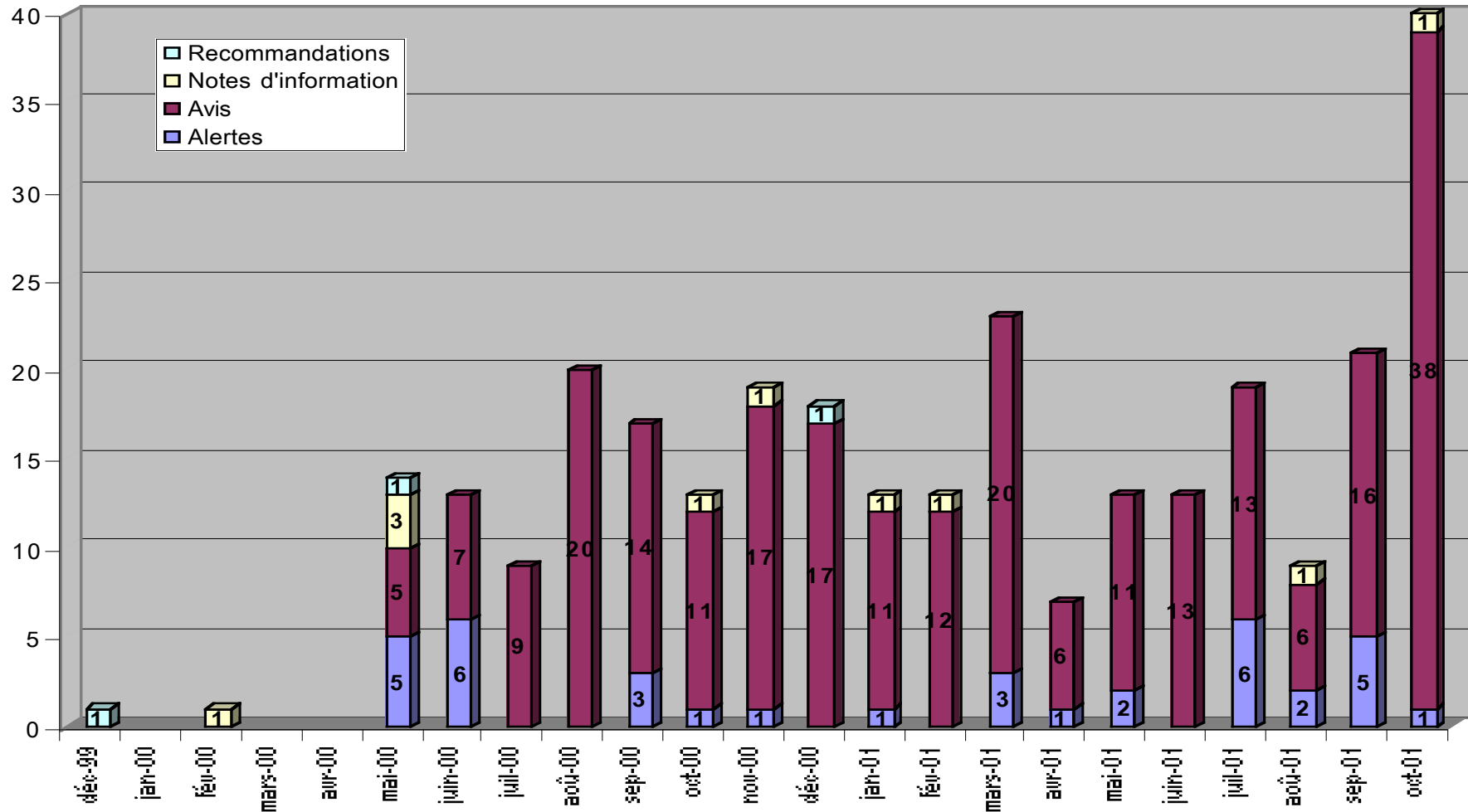
Constituency

- French administration community: all French public offices and services as well as local and territorial offices
(the root is * .gouv.fr)
- CERTA is not a provider

Publications

- CERTA publishes four kind of documents:
 - “**AVIS**” (Advisories) gives a brief description of a vulnerability, its consequences for security and the way to protect the system (patches);
 - “**ALERTES**” (Alerts) are specific advisories for witch patch are not provided yet;
 - “**NOTES D’INFORMATION**” (Information Notes) are more detailed advisories;
 - “**RECOMMANDATIONS**” (Recommendations) suggest appropriate measures to face specific computer threat.

Publications: Statistics



Resources

- Four networks:
 - “**Internal Network**”: publication tools, incident handling, tools development, vulnerabilities database, ...
 - “**Public Network**”: web site, mail server and DNS
 - “**Surf Network**”: Internet access
 - “**Test Network**”: set of easily re-configurable computers (OS, connectivity, ...)

Tools

- Incident Handling: **GNATS** (the GNU Bug Tracking System)
- Forensics: open sources tools and CERTA tools
- Web server (“Internal Network”): search engine on vulnerabilities, interface to GNATS, email archive, ...
- Publication version control: **CVS**

How to join CERTA

- *Telephone:* (+33) 1 41 46 25 23 ¹
(+33) 1 71 75 83 00 ²
- *Fax:* (+33) 1 41 46 37 01
- *E-mail:* CERTA-svp@certa.ssi.gouv.fr
- *WEB:* <http://www.certa.ssi.gouv.fr>

¹ Direct call during business hours
(Monday-Friday, 08:30 - 18:30, GMT+0100/0200 DST)

² 7/7 - 24/24 (outside business hours) in French only!