



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

STATE INFORMATION SYSTEM SECURITY REINFORCEMENT PLAN (2004-2007)

10 March 2004

CONTENTS

1. INTRODUCTION	2
2. FOUR OBJECTIVES	4
2.1. Secure Senior Authority transmission means	4
2.2. Secure government information systems	4
2.3. Set up operational capabilities to respond to computer attacks provided for in the plans.....	4
2.4. Include our information system security policy within the scope of our security policy in the European Union.....	4
3. TWELVE MEASURES	5
3.1. Training and skills	5
3.2. Organisation.....	7
3.3. Equipment.....	9
3.4. Industrial fabric.....	11
3.5. Legal framework.....	13
4. IMPLEMENTATION	13
APPENDIX 1: LETTER OF INSTRUCTION	17



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

1. Introduction

For some years now, the annual ministerial departments' reports on the status of information system security (ISS) indicate ongoing difficulties in improving the situation: insufficient and isolated operational skills and capabilities, lack of decision-makers' awareness of the stakes involved, insufficient duly qualified security products combined with monopoly positions in significant market sectors, proliferation of non-secure network interconnections¹, national regulations that are difficult to enforce, poorly coordinated European dimensions. While some individual improvements have been observed, the work completed, whatever commendable it may be, has been unable to keep up with rapid developments in technologies and threats.

The events of September 11, 2001 led to a review of all vigilance and intervention plans with respect to terrorist risks. The hitherto absent information system security component has been introduced. The awareness of the need for the rapid control of all the operational circuits concerned has also increased.

The governmental Program "RE/SO 2007" plans to take a step further in e-government. The success of the strategic plan drafted for this purpose by the ADAE² will essentially be based on the ability of correspondents to master the technology and authentication procedures, to ensure the integrity of the data exchanged and to respect confidentiality.

A comparison with similar countries demonstrates the diversity of information system security organisations, regulations and practices. In the long term, European harmonisation appears to be necessary.

In a letter dated 4 April 2003 (see appendix 1), the Director of the French Prime Minister's department instructed the ministerial departments and the General secretariat of national defence to prepare a specific plan of action by October 2003 to "secure the main central and local governmental networks, and those used for vital infrastructure management".

This plan of action, entitled the "State information system security reinforcement plan" was sent to the Prime Minister's department on 17 October 2003. It was discussed and approved at an interministerial meeting on 16 December and incorporated in the e-government programme (ADELE programme) in turn approved at an interministerial meeting on 23 December.

The reinforcement plan proposes 4 objectives (section 1) and 12 measures divided into 5 areas (section 3)³. The lack of resources currently available in a number of ministries and the difficulty in precisely addressing all the issues involved has led to the recommendation to conduct the action in two phases.

A first phase will consist of building, in three years, a solid base addressing the objectives set at a first level (section 4). On this basis, it will be possible to evaluate the resources required for a second phase in the medium term more specifically, resulting in more complete and long-term protection of the State's information systems.

¹ A map of the rollouts and interconnections of sensitive networks has yet to be drafted, within the scope of the vital infrastructure inventory initiated in 2002.

² The specific aims of the ADAE Strategic e-Government Plan are to dematerialise remote procedures (100%), exchanges between users and state departments (66%) and between state departments (100%) by 2007.

³ In the ADELE programme, the 12 measures are grouped together slightly differently into 4 areas: "pooling of departments" including the measures O1 (with the exception of joint organisation for product development), O2, O3 and J1; "skills development" includes F1, F2, F3; "security product provision" includes joint organisation for product development (taken from O1), E2, I1, I2 and F4; "product acquisition" corresponds to E1.



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

In his speech on 9 February 2004, made in Lyon on the occasion of the launch of the ADELE programme, the Prime Minister made the e-government action plan and the reinforcement plan official with the planned funding: 1.8 billion Euros, one tenth of which is to be allocated to the reinforcement plan (see section 4).



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

2. Four objectives

2.1. Secure Senior Authority transmission means

It is essential for Senior Authorities to have completely secure communication means on a permanent basis to contact their main national and international correspondents, along with certain interministerial networks reserved for the most senior ministerial officials.

This objective relates to all standard communication means: telephone lines (in offices or during trips) and mobiles, faxes and e-mail systems. Even though a low volume is involved in this market, it is very demanding in terms of quality.

The objective is to ensure, under all circumstances, the security of all protected communication means for the use of Senior Authorities, based on supervision under the direct control of state authorities.

2.2. Secure government information systems

At the present time, very few ministries have a specific document detailing their information system security policy. The reinforcement plan must aim to:

- secure the new e-government functions, in accordance with the ADAE strategic plan and guidelines.
- explain security policies and initiate corresponding action plans in terms of organisation, human potential and material and financial resources.

2.3. Set up operational capabilities to respond to computer attacks provided for in the plans

The diversity of the possible targets and the speed of the propagation of computer attacks require reactivity and efficiency.

The objective of the reinforcement plan in this case is for the measures provided for the Piranet and Vigipirate plans to become fully operational, with

- by the end of the first quarter in 2004, the definition of ministerial versions of the Vigipirate SSI and Piranet plans;
- by the end of 2004, the availability of operational resources corresponding to these ministerial plans (availability of secure links under all circumstances, directory of correspondents, full control by all parties involved of the measures to be applied, availability of teams that can be mobilised without delay and capable of conducting a round-the-clock long-term operational programme).

2.4. Include our information system security policy within the scope of our security policy in the European Union.

The French strategy in terms of defence and security is defined in a European perspective. Its information system security version must also be clearly defined in this perspective. To this end, the role of the work of the Council and Commission, in terms of regulatory and institutional aspects, remains a priority, as is the involvement of French personnel in the European structures responsible for these issues.

With respect to the operational aspects, these guidelines must result in a pooling of tools, the interconnection of operational chains and the implementation of mechanisms enabling more efficient crisis and incident management on areas which, by their nature, are not restricted to a national scope. This policy should make it possible to offer economic players greater prospects and favour, within the Union, a broader incorporation of information system security issues.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

3. Twelve measures

To meet the objectives set, the measures to be taken are broken down into five areas:

- Training and skills
- Organisation
- Equipment
- Industrial fabric
- Legal framework

3.1. Training and skills

Although it makes use of very elaborate technology, information system security is nonetheless based on the skills of the men and women involved: particularly information system security specialists and experts, but also the users, who are directly concerned, and the decision-makers, whose role is essential to ensure the acceptance, or implementation, of good practices and resource allocation.

Therefore, the development of information system security skills, within state departments and with trusted service providers is a key factor. The purpose of four measures proposed below is to meet this requirement.

MEASURE F1: DEVELOP INFORMATION SYSTEM SECURITY SKILLS WITHIN STATE DEPARTMENTS

The lack of competent information system security specialists in state departments has become particularly alarming. Therefore, the acquisition of new skills and the ongoing refreshing of those available are required urgently for all state departments. This results in considerable requirements in terms of training and awareness.

In quantitative terms, the actions and resources in place⁴ cannot keep up with these requirements despite the quality of the work accomplished.

Therefore, it is proposed to set up an interministerial information system security training plan. Multidisciplinary by nature (scientific, technical, legal, economic), this plan will include study allocations to encourage vocations at a very early stage, and a reinforcement of continuous training, making maximum use of online learning. A particular effort will be made for students headed for careers in state departments. To this end, an agreement will be signed between the SGDN information system security training centre, the ministry of National Education and the Minister of Labour (professional training).

Moreover, in an employment market that is and will remain stretched in this area, it is necessary to take all necessary measures to retain the skills acquired in this way. Therefore, it is proposed that these skills should be recognised and valued in professional terms, by means of a suitable remuneration system and career paths based on merit.

MEASURE F2: REGULARLY CONDUCT EXERCISES IN ACCORDANCE WITH THE INFORMATION SYSTEM SECURITY PLANS

Attacks targeting information systems are characterised by their untimely activation, their ubiquity and the speed with which their effects are propagated. A terrorist computer attack may

⁴ particularly the SGDN/DCSSI ISS training centre (CFSSI), the website ssi.gouv.fr, the DCSSI's protected reserved access site for state departments, etc.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

also involve potential damage that is incomparable with the already considerable damage of everyday attacks intended as jokes or for the purpose of crime. Therefore, it is important that all the departments concerned are able to react without delay and hesitation when faced with an attack on the State's information systems. It must be possible to apply and implement information system security plans instantly.

To achieve this, an interministerial and ministerial department exercise programme and policy⁵ is required. A quarterly frequency is envisaged for all these exercises.

Single-themed interministerial exercises, which are simple and mobilising for state departments, will be targeted on specific objectives and will attempt to test the liaison chains, on the one hand, and the implementation of the intervention plan and the control by the various parties involved of the actions under their responsibility, on the other. Other interministerial exercises, on a national or international level, particularly on a European level, will make it possible to activate all the chains of command and decision-making; they will account for aspects related to crisis communication and communication to populations and will test the implementation of procedures associated with international cooperation.

On a ministerial level, the capability of the operational units to deal with computer attacks will be evaluated, along with the suitability of the resources available. The DCSSI may be consulted if required to assist the organisers of these ministerial exercises.

MEASURE F3: INCREASE AWARENESS OF SENIOR OFFICIALS

Experience proves that, for many senior officials, information system security is a matter for the experts. This is due to the fact that this discipline is apparently very technical and also that the threat appears to be very diffuse and theoretical.

However, the action of senior officials is decisive to favour, if only by example and as an impetus, or, if required, to impose the spreading of restrictive good practices which are frequently perceived as being unjustified.

To convince these senior officials (cabinets, central departments) and organisations in charge of vital infrastructures of the genuine nature of the threats and also of the possibility of protection, a periodical awareness programme will be proposed, for instance at a rate of three to four half-day seminars per year, to discuss the main aspects of information system security: threats, possible responses, resources required, international context, action schedule⁶.

MEASURE F4: QUALIFY PRIVATE INFORMATION SYSTEM SECURITY CONTRACTORS

Outsourcing can contribute to improved control of public expenditure and will therefore be favoured for functions which are not regalian in nature, provided that suitable levels of skills and security are guaranteed.

Therefore, it is proposed, initially, to conduct an inventory of the qualification processes for the information system security sector. This inventory will be conducted in consultation between the

⁵ The first ISS exercises, conducted in May and September 2003, and then in February 2004, have already demonstrated the potential benefits of this type of measure.

⁶ A first seminar, focusing on ISS threats, was organised by the SGDN in October 2001 for ministerial cabinet members.



PREMIER MINISTRE

public sector and the private sector, under the aegis of AFNOR⁷, or the European standardisation committee. It will account for projects in progress in this area.

On this basis, contractor qualification procedures will subsequently be defined⁸. They should be operational for INFOSEC Advisory Services and Audit and Detection activities by 2006. In addition, it will be necessary to ensure that this contractor qualification may be required for public sector contracts.

3.2. Organisation

MEASURE O1: REINFORCE THE ORGANISATION OF INFORMATION SYSTEM SECURITY WITHIN MINISTRIES AND EUROPEAN INSTITUTIONS

The incorporation of governmental objectives with respect to ISS must be effective at all levels of state departments in terms of objectives, organisation and resources.

It is proposed that each ministerial department encountering difficulties in the security of its information systems should analyse, with respect to governmental objectives and its own security stakes and objectives, the optimal distribution of the various generic functions in this area within its organisation, and define and initiate an adjustment plan without delay.

The drafting of guidelines accounting for information system security⁹ will make it possible to succeed in such an analysis¹⁰ and develop such an adjustment plan.

At the present time, the ability to steer such an approach is frequently lacking in ministries. The first step will consist of setting up a minimal team capable of taking on this steering, assisted by external support (DCSSI, private contractors) as required.

In addition, an improved transfer of the national information system security policy within the scope of our security policy within the European Union requires marked involvement of French experts in the European structures in place.

Therefore, particular importance will be assigned to the secondment of French experts to the European Network and Information Security Agency (ENISA), which was created the 14th of March 2004, for 5 years, by the regulation of the European parliament (EC) N°460/2004 and of the council dated 10 March 2004.

MEASURE O2: ENSURE OPERATIONAL DUTIES IN THE EVENT OF APPLICATION OF THE PIRANET AND/OR VIGIPIRATE PLANS

The Vigipirate plan, at the red and scarlet levels, and the Piranet plan provide for the set-up of round-the-clock operational centres at the SGDN and in the ministries.

Therefore, it is necessary to guarantee the availability, under all circumstances, of sufficient competent human resources to form these operational teams in the SGDN coordination centre and in the ministerial crisis centres.

⁷ Association Française de Normalisation

⁸ based, for example, on Information Technology Security Evaluation Centre (CESTI) approval, as specified in the decree 2002-535.

⁹ The DCSSI provides all requesting ministerial departments with technical support on the drafting of master plans, particularly for the identification of the functions to be carried out.

¹⁰ In some ministerial departments, an ISS master plan already exists or a more general master plan (IT master plan or security master plan) already handles ISS aspects in a manner that, in practice, has proven to be satisfactory.



PREMIER MINISTRE

At the present time, existing personnel is not always sufficient to form, even during working hours, the complete operational teams¹¹ stipulated by the plans. The extra personnel, mobilised exceptionally, should be obtained from new resources set up to carry out other measures of the reinforcement plan, taking care to adapt skills to the operational specificities.

MEASURE O3: POOL A SET OF INFORMATION SYSTEM SECURITY ORGANISATION

Pooling departments is a pragmatic way to meet the common needs of ministries, while decreasing public expenditure and optimising human resources. The following actions will contribute thereto:

Set up a joint security product development unit

State department requirements that cannot be met by commercial products must be covered by an organisation capable of defining common requirements, handling priorities, drafting specifications, mobilising the corresponding budgets, placing and following up contracts and implementing cost-effective acquisition procedures¹².

Such a unified organisation will be set up with the support of the CISSI¹³ (expression of common requirements, breakdown of budgetary contributions, priority development plan) and the ministry of defence (completion of high-security product development and acquisition projects, design of encryption algorithms and status control of component and product design resources). The technical specifications corresponding to the desired security levels will be drafted in consultation between the competent departments of the ministries and SGDN. The equipment qualification work will be the responsibility of authorised teams (see below).

The set-up of this joint unit organisation will require a review or amendment of certain regulatory texts¹⁴.

Coordinate ministerial public key infrastructures (PKI)

The availability of keys authenticating the parties involved in ministries, which are interoperable between ministries, is an essential step in the development of e-government¹⁵.

An interministerial public key infrastructure will be set up to enable dialogue between and with the various ministerial departments.

Subject to a request from several ministries, it should be possible to provide them with a pooled public key infrastructure.

Organise interministerial feedback

Monitoring and alerts are vital functions for incident resolution, particularly for the activation of vigilance and intervention plan measures at the right time. The analysis of interfering signals on networks is currently conducted in an empirical and dispersed manner.

¹¹ network monitoring, incident management, response to attacks, etc.

¹² as has been carried out, for example, in the Netherlands

¹³ Information Systems Security Interministerial Commission

¹⁴ particularly interministerial directive 4201 and interministerial instruction 77/CD dated 13 April 1995, which assigns the ministry of defence with a "management" responsibility for the development of equipment intended to protect "governmental information systems" (i.e. "handling classified State information (defence, diplomacy, State security)").

¹⁵ see in particular the Strategic Plan of the E-Government Development Agency (ADAE).



PREMIER MINISTRE

A significant operational gain will result from the set-up of pooled knowledge and incident reporting and the harmonisation of procedures, terminology and work methods.

Harmonise interconnection ministerial gateway management

The operation of interconnection gateways is particularly demanding in terms of human resources while requirements increase with network development.

Initially, it will be necessary to audit the various gateways of the ministries¹⁶ and then harmonise their operating and organisation methods.

A suitability and feasibility study will then be conducted with a view to a bid for the remote administration of the gateways harmonised in this way. This pooling may comprise the administration of a common Internet access gateway, completed if required by continuous Internet monitoring.

Set up an information system security training and INFOSEC advisory structure for prefects of defence zones

These zone-based structures must render support actions easier to access for decentralised departments and also improve reporting of precursor signals of incidents, thus reinforcing the ability to initiate vigilance and/or intervention plans at the right time.

These structures, set up with the zone prefects, will have a confirmed interministerial role, given that the activities and practices of each decentralised ministerial department will remain under the responsibility of the corresponding central departments.

The set-up of two local teams (Eastern zone and Western zone) has made it possible to acquire experience and an organisation model (at least two people per structure).

The proposed action consists of extending the zones covered progressively at a rate of one to two structures per year.

3.3. Equipment

MEASURE E1: ACQUIRE A SERIES OF PRIORITY EQUIPMENT

The State's ISS reinforcement plan comprises a significant effort to acquire infrastructures and technical resources adapted to the new stakes involved in information security. This effort is broken down into three sections

Renewal of the State's own resources for the security of its communications and the continuity of its action in the event of a crisis.

First of all, it is essential to ensure a desirable level of security for the protected communication means provided to senior authorities and to maintain that level of security over time, in line with the following objectives:

- protection of information from any threat to its confidentiality or its integrity;
- continuous availability of resources;
- easy and ergonomic access;
- interoperability between the different systems;

¹⁶ these gateway audits have started in several ministries.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

- operation in fixed or mobile mode;
- projection capabilities within very short timeframes (a few hours).

Several projects will be initiated within this scope.

The reorganisation of the planning architecture (vigilance and intervention plans, backup plans, specialised plans) and the exercise doctrine requires the reinforcement of governmental crisis communication systems. Reliable and available under all circumstances, these systems must be able to route information very rapidly with guaranteed integrity and confidentiality consistent with the particular requirements of the crisis situation.

The Rimbaud network will be maintained at a high security level, particularly with respect to encrypted telephony. It should be associated with a secure governmental e-mail system. It should be possible to interconnect it with specialised ministry networks. To this end, the CTG (Governmental Transmissions Centre) interconnection gateway will be upgraded in order to provide an interconnection for secure national e-mail systems (governmental and ministerial: Interior, defence, Foreign affairs) and controlled access to systems of the same security level of the EU and NATO, under more effective conditions.

Secure new e-government tools

E-government will only keep all its promises if it inspires confidence in the various parties involved, on the basis, in particular, on mutual identification capabilities with no possible ambiguity and authentication capabilities for the e-mails exchanged. Therefore, it is proposed to consider the allocation of a professional card with an electronic signature and "high" authentication capabilities to each public servant as a priority¹⁷.

It will also be necessary to develop tools enabling an interministerial public key infrastructure management to carry out mutual recognition of the signatures of the various ministerial departments (dating, ministerial policy key management comparison, valid key and revoked key publishing tools, etc.). This will make it possible to set up management of access rights for the various parties involved to the various types of data (access right management).

To complete the e-government requirements, it is finally proposed to develop electronic signature tools corresponding to the different levels of confidence required¹⁸. Particular efforts will also be conducted for the development of specific tools and architectures to secure the interconnection of inter-state department networks (security of the AdER network in particular).

Acquire or develop network design, security and monitoring tools

The acquisition of a consistent range of tools to monitor and audit the security of networks and systems and their progressive integration into national infrastructures should give the State and its domestic and international partners a sufficient guarantee of their defence and response capabilities in the face of new threats to the integrity, availability or confidentiality of these infrastructures. In a number of ministries, particular efforts should be devoted to completing or renewing filtering or encryption equipment installed bases.

¹⁷ The deployment of electronic national identity cards (CNIE) with the same capabilities is also a project of primary importance, but does not fall within the scope of the State information system security reinforcement plan.

¹⁸ As defined in the Intersectorial Referencing Policy for Security (PRIS) – www.adae.gouv.fr



PREMIER MINISTRE

MEASURE E2: RAPIDLY INCREASE THE NUMBER OF QUALIFIED SECURITY PRODUCTS

The qualification of a security product (in a three-level scale: standard, reinforced and high) is the result of its ability to withstand threats of different degrees. This qualification is based on the adoption of technical specifications presumed to be representative of the resistance to a certain threat level, on a recognised evaluation of compliance with these specifications, and on the level of confidence which could be established with respect to the design and development teams¹⁹.

These new rules must make it possible to increase the range of qualified products rapidly, provided that the technical specifications associated with the various levels of threats are available and can be incorporated into the product design by trusted contractors.

The proposed measure consists of drafting, for the different types of products and security levels, technical specifications based on the evaluation of existing products and R&D work, particularly that defined by the coordination structure set up by the Interministerial committee for the information society (CISI meeting dated 10 July 2003²⁰). European cooperation will make it possible to broaden the scope of the work²¹.

Consultation with the industrial sector²² will precede the validation of these technical specifications with a view to incorporation in invitations to tender for public contracts²³.

For the reinforced or high levels, particularly equipment protecting confidentiality, the consultation will be limited to some trusted manufacturers and the specification will be protected, or even classified.

An important factor of the system will be the definition of an interministerial cryptographic policy specifying which type of cryptographic algorithm can be used to which category of users. In correlation, an action will be conducted to obtain reference cryptographic libraries and place them at the disposal of manufacturers.

3.4. Industrial fabric

MEASURE I1: ENSURE DIVERSITY IN SECURITY PRODUCT PROCUREMENT

In the face of an information technology market characterised by dominant positions in both software and hardware, a series of actions aims to maintain diversity in security product procurements.

¹⁹ see the new ISS doctrine guideline, approved by the Prime Minister's department in Autumn 2002 (N°1884/SGDN/DCSSI/DA/E/DR dated 3 October 2002).

²⁰ CISI 4 (creating a climate of confidence/acting on supply); a structure placed under the aegis of the Ministry of Research and Industry will define the priority areas in the field of R&D in information system security.

²¹ a first cooperation of this type has been envisaged with Germany (BSI), the Netherlands (NLNCSA) and France (DGA, DCSSI), on the SINA workstation security project.

²² a public seminar was held at the Military College in February 2002 on PKIs. A workshop open to manufacturers was organised by the SGDN on 16 September 2003 on interconnections.

²³ for example, in the form of approved standards in accordance with AFNOR (decree 84-74 dated 2 January 1984).



PREMIER MINISTRE

Stimulate the development of innovative industrial products meeting identified requirements, by favouring the incorporation of technical specifications corresponding to the standard level of security, either in the design of new products or in the adaptation of existing products. This approach includes support for stages prior to product industrialisation (prototypes, pre-series, evaluation work).

This action will be aimed at a trustworthy industrial fabric, which it will continue to maintain and extend, particularly with SMEs.

To grant "State approved investment subsidies" and/or "repayable advances", it is proposed to identify an interministerial fund, managed by the SGDN according to the guidelines set by the CISSI.

Promote the development²⁴ and use of freeware within state departments

Freeware offers an interesting alternative to the dominant positions acquired by certain products for which manufacturers own all the rights.

Avoid the consolidation of dominant market positions, and particularly the emergence of exclusion mechanisms.

Relations with manufacturers enjoying considerable dominant positions will be limited to technical contacts to improve the knowledge of their products and the associated risk and provide state departments with guides of good practices, while warning the manufacturers against any hegemonic approach.

MEASURE I2: ADAPT EVALUATION AND CERTIFICATION CAPABILITIES TO REQUIREMENTS

Evaluation/certification, currently covered by the decree 2002-535, is an essential component of product qualification.

Lethargic for a long time, the evaluation/certification sector has been experiencing strong growth in recent years which requires an adaptation of structures and capabilities. This consists of creating the conditions which could make it possible, by 2007, to impose the acquisition of evaluated and certified security products for state departments.

Adapt evaluation standards and develop the skills of the Information Technology Security Evaluation Centres (CESTI)

The use of new evaluation standards, particularly on the other side of the Atlantic²⁵, is leading to an increasing number of French suppliers having their products evaluated outside the country. So that national teams remain recognised in terms of evaluation and certification, these standards must be mastered by the evaluation teams (recognised private contractors such as CESTI²⁶) and the certification bodies (Certification centre based at the SGDN).

²⁴ with contributions from teams and public servants, subject to a clarification of the legal conditions.

²⁵ such as FIPS 140-2 or Federal Information Processing Standard: Security requirement for cryptographic modules

²⁶ Information Technology Security Evaluation Centres, which are private bodies approved by the Certification Centre.



PREMIER MINISTRE

Whenever possible, CESTI qualification will also be extended to the team and personnel clearance so that they can take part in product evaluation with a view to protecting classified information.

Revise the organisation of the certification activity

Certification is currently conducted by a single state department based at the SGDN (Certification centre). To meet the growing demand for certificates, without increasing the workloads of state authorities, it is necessary to distribute certification capabilities within structures combining management flexibility and control of a sensitive activity.

This could be obtained for example by delegating a certification responsibility to another state department or a supervised organisation, in technological areas in which they are already specialised.

Better use of compromising signal measurement capabilities

Reserved for the protection of classified information for a long time, this activity requires heavy investment. Entirely under state responsibility (DGA/CELAR, SGDN/DCSSI), it is now suffering from a delay in the rationalisation of the resources in place, while the development of wireless connections is increasing signal measurement requirements.

The action will consist, through improved human resource management, of finding gains in productivity by optimising the use of existing measurement resources (CELAR, DCSSI and some ministerial departments). It will also consist of examining the possibilities of sharing, or even pooling, this activity with certain national or European partners.

3.5. Legal framework

A set of legislation and rules (laws, codes, interministerial instructions, directives, guides) forms the legal framework for information system security. The new guidelines of the doctrine of Autumn 2002²⁷ and the implementation of the above measures now require a review of some of these documents in order to complete it (scope of system approval, product approval procedure) or to amend it (unified security product development organisation, product qualification).

MEASURE J1: ADAPT REGULATORY TEXTS TO THE NEW CONTEXT

The proposed measure will involve explaining the interministerial information system security policy and giving it a consistent and solid regulatory base, so that each ministerial department can deduce its own security policy for its specific framework.

This work will be conducted under the aegis of the CISSI, for example, in the form of a specific working group, based, if applicable, on studies conducted by outside contractors.

4. IMPLEMENTATION

In view of the current situation, the ambition of the selected objectives for the reinforcement of the State's information system security makes it very difficult to set a precise estimation of the resources required: only an analytical approach conducted in each of the ministerial departments, particularly in the form of a master plan, can provide such information. However, in many cases,

²⁷ No. 1884/SGDN/DCSSI/DA/E/DR dated 3 October 2002.



PREMIER MINISTRE

the lack of qualified personnel, delays in the inventory of sensitive systems and applications and the weakness of the organisation do not permit this.

Therefore, it is proposed to proceed in two stages:

- firstly, initiate the proposed measures by mobilising a volume of resources corresponding to the first core of objectives. This "hard core" of the reinforcement plan should make it possible, in three years, to obtain significant results and determine the requirements for complete implementation of the plan in all the departments;
- subsequently, on the basis of the experience acquired and new estimations, allocate the additional resources to systematically increase the level of security of the State's information system, in accordance with the stipulated objectives.

For each of the five areas of measures, it is possible to specify the resources to be mobilised over the period from 2004 to 2006 and the expected results.

In terms of skills development, 5 million euros and 5 positions will be necessary to control the vigilance and intervention plan application procedure, to define INFOSEC Advisory and Audit and Detection activities contractor qualification procedure, to stimulate information system security career choices and to develop a significant training effort.

In terms of organisation, the hard core represents about sixty positions (full-time equivalence) within ministries, a dozen interministerial positions and a cost of around ten M€ over the period. This effort should make it possible to draft master plans wherever they are required, ensure a first level of reinforcement of support and monitoring capabilities with the ministries, confirm the presence of French experts within bodies in the European Union devoted to information system security and set up a series of pooled organisations (for product development in particular).

In the event of the initiation of the red/scarlet Vigipirate or Piranet plans, these human resources will make it possible to mobilise the minimum operational capabilities required over time in the central departments.

Security equipment acquisition represents the highest cost of the proposed plan. A sum of € 151M over the period aims to cover upgrading and security requirements for the State's essential means of communication.

Security products	Cost (M€)
Communication of senior authorities Secure gateways Dedicated encryption resources RIM	5
Crisis connections Perpetuation of Rimbaud Secure e-mail system Gateways	28
Defence equipment Smart card authentication Incident detection and tracking	55
MISILL equipment Network scramblers Public servant card	33
Equipment for other ministries	30



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

At the same time, significant action must be initiated (€ 8M, 10 interministerial positions) to increase the number of security products.

This renewal and extension of the security product installed base should make it possible to improve the security of senior authority transmissions. They will also create increased confidence in the new stages of e-government, improve vigilance and intervention plan initiation conditions and reinforce France's position in the European context.

The consolidation of the industrial fabric will require expenditure to stimulate innovation and control new evaluation standards (representing € 12M) and 17 positions at an interministerial level (signal measurements, certification work, freeware promotion). This should make it possible to ensure the diversity of security product procurements and their quality control, while controlling the corresponding workload for the public authorities.

Finally, the adaptation of regulatory texts to the new context will help implement most of the measures and make a general contribution to the objectives to be met. Since it does not require any noteworthy new resources, this measure belongs to the hard core proposed to initiate from 2004 to 2006.

Summary of resources required to implement the first stage of the reinforcement plan over three years

Resources	Training/ skills	Organisation	Equipment	Industrial fabric	Total
Interministerial ²⁸ positions	5	13	10	17	45
Ministerial positions	0	62	0	0	62
Cost (M€)	5	10	159	12	186

The summary of the resources corresponding to the hard core of the reinforcement plan demonstrates a cost of the order of € 186M over three years with some one hundred full-time equivalences (FTE) to be distributed between the various ministerial departments (62 FTE) and the interministerial departments (45 FTE).

To a certain extent, the new ministerial human resources may consist of subcontracting or be obtained from the redeployment of existing skills. Some budgetary allocations may also be obtained from redeployments stemming from improved incorporation of security in development projects.

Finally, it is planned to set up tools to monitor the allocated resources (existing and new) and progression towards the objectives of the reinforcement plan. In particular, management charts, currently under preparation, will enable each ministry to perform its own monitoring (indicators) of investments (human, material, financial). A reference system will be proposed for these ministerial management charts so that they facilitate the preparation of a summary (for example, for the annual report intended for the Prime Minister) and a regular evaluation of the progress of the reinforcement plan.

²⁸ expressed as "full-time equivalences"



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Appendix 1: Letter of instruction

PREMIER MINISTRE
—
LE DIRECTEUR DU CABINET

Le 04 AVR. 2003

LE PREMIER MINISTRE

À

MESDAMES ET MESSIEURS LES MINISTRES ET SECRÉTAIRES D'ÉTAT
A l'attention de Mesdames et Messieurs les Directeurs de Cabinet

MONSIEUR LE SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE NATIONALE

Objet : Sécurité des systèmes d'information.

La sécurité des systèmes d'information de l'Etat est un enjeu de première importance pour les pouvoirs publics. Elle doit faire l'objet d'une attention particulière de la part des autorités ministérielles.

Le rapport que m'a transmis le Secrétaire général de la défense nationale, sur ce dossier, et dont vous avez été rendus destinataires pour la partie qui concerne votre département, dresse un constat préoccupant. Si certains progrès sont signalés, les vulnérabilités demeurent, voire s'accroissent. Certains départements ministériels n'ont en effet pas encore mis en place de chaîne de responsabilité opérationnelle en ce domaine ; les inventaires de réseaux à caractère sensible restent très incomplets ; peu de schémas directeurs existent, ni même sont en cours d'élaboration ; enfin, les personnels nécessaires à cette fonction font défaut au sein des administrations centrales.

Or, trois facteurs viennent donner une acuité supplémentaire à ce sujet :

- le passage à la deuxième phase de l'administration électronique, celle de la dématérialisation des procédures, ne sera possible que sur la base d'une confiance partagée, entre administrations et administrés ;
- une nouvelle étape de la construction européenne est engagée, caractérisée par l'ouverture généralisée sur la société de l'information, ainsi que par de nouvelles dimensions géographiques et politiques ; il est indispensable, que ces échanges soient, à terme rapproché, entièrement sécurisés ;



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

- enfin, les systèmes d'information, sur lesquels repose le bon fonctionnement de nos infrastructures vitales, apparaissent comme une cible particulière, au regard du terrorisme. A ce titre, le nouveau plan Vigipirate définit des actions de protection, qui visent à sécuriser rapidement, les systèmes d'information prioritaires et essentiels de l'Etat.

Le Premier ministre demande, donc, qu'un plan « sécurité des systèmes d'information de l'Etat » soit engagé dans les plus brefs délais pour sécuriser les principaux réseaux gouvernementaux, aux échelons centraux et locaux, ainsi que ceux utilisés pour la gestion des infrastructures vitales.

A court terme, il s'agira d'assurer les liaisons entre tous les responsables opérationnels, ainsi que de renforcer, si nécessaire, les chaînes fonctionnelles.

A moyen terme, il conviendra d'aboutir à une prise en compte généralisée des questions de sécurité, par les administrateurs et les utilisateurs des systèmes d'information. L'objectif final sera de disposer, au plus tard en 2006, d'une gamme étendue d'équipements de haute sécurité et d'une réglementation harmonisée dans un cadre européen.

Sur la base de l'analyse de la situation dans les administrations, dont vous avez la charge, je vous demande, par conséquent, de répertorier sans délai, les données, les applications informatiques et les réseaux à protéger. Vous élaborerez un plan sur trois ans, visant à assurer leur sécurité. Il portera sur le renforcement des chaînes fonctionnelles et des liaisons opérationnelles, l'établissement d'un schéma directeur et d'une politique de sécurité, le développement des compétences, l'identification des types d'équipement de sécurité à acquérir. Ce plan devra inclure, si nécessaire, les besoins des services déconcentrés et les échanges existants ou prévisibles à l'échelle européenne. Il fournira, enfin, une estimation des ressources humaines et budgétaires nécessaires à sa réalisation.

Par ailleurs, je donne instruction, au Secrétariat général de la défense nationale, de mener un travail équivalent, pour ce qui concerne les réseaux interministériels.

Enfin, une synthèse de ces plans ministériels et interministériels sera élaborée dans le cadre de la Commission interministérielle pour la sécurité des systèmes d'information, de façon à constituer un plan global. Je souhaite que ce plan me soit soumis d'ici le 1^{er} Octobre.

Vous ne manquerez pas de me tenir informé de toute difficulté rencontrée, dans l'application de ces instructions.



Pierre STEINMETZ

