The enforcement of NATO INFOSEC requirements into the policy and architecture of CISs

Frantisek Vosejpka
frantisek.vosejpka@i.cz
S.ICZ a.s.
V Olsinach 75
Prague 10, post zip 100 97

Abstract
A series of national problem-oriented communication and information systems (CISs) have been developed within certain Czech government organizations and focused mainly on the Czech Restricted security level. A few of these CISs have received approval to operate at target-classification level, but only within the local networks. The other CISs are operated without completion of required security measures and therefore handle only unclassified information. The certification and accreditation processes of these CISs have failed to succeed due to a current lack of financial resources and skilled personnel. In both cases these CISs do not meet predetermined network functionality. This situation, in conjunction with a reduction in IT specialists in the government sector necessitates a series of fundamental decisions to enforce revised NATO INFOSEC policy requirements into CISs of the Czech Ministry of Defence (MoD) and partially the Ministry of Foreign Affairs (MFA). Numerous problem-oriented CISs have to be reduced to a small number of overarching CISs with all required Functional Area Services. There is a necessity to realize the current state and resource limitations, to set out new operational requirements for the functionality of CISs, to set out a new target system and service architecture, life cycle phases and steps with priorities and terms capable of guaranteeing a smooth transition from the current to the target state. The security within this process must be seen as added value and must be reflected from the very beginning, otherwise serious barriers will arise, which will cause failure to meet security and operational requirements. Simultaneously the project risks that have caused failure to certify current CISs (lack of communication security and excessive system building before system certification) have to be eliminated.

Keywords: NATO, INFOSEC, CIS, security, policy, directive.

1 Introduction
The communication and information systems (CISs) within the Czech Republic that handle the classified information are subject to certification by the Czech National Security Authority (NSA) before handling the classified information. The objective of this article is to sum up the breaches that have caused a situation whereby the CISs of some Czech government organizations (typically the Ministry of Defence (MoD)) have not reached the required functionality and have failed their certification process. A further objective is to illustrate the legislative requirements stated by Czech Act No 148/1998 of the Collection of Laws (Coll.) on “Security of Classified Information” [1] and revised NATO Security Policy [2] that concentrates its requirements into the INFOSEC area. And finally to introduce possible features of target CIS INFOSEC architecture and migration steps to such a target state.

The content of this article is unclassified and limited by quite weak access of a civil firm (with security clearance) to the whole suite of NATO Security Policy documents.

2 Applicability of NATO INFOSEC policy within the national conditions
The Enclosure F “INFOSEC” of NATO Security Policy [2] sets out the policy and minimum standards for the protection of NATO classified information, and supporting system services and resources in communication, information and other electronic systems handling NATO classified information. The document defines INFOSEC as “the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability,
whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. In order to achieve the security objectives of confidentiality, integrity and availability for classified information stored, processed or transmitted in communication, information and other electronic systems, a balanced set of security measures (physical, personnel, security of information and INFOSEC) shall be implemented to create a secure environment in which to operate communication, information or other electronic systems.”

The “Primary Directive on INFOSEC” [4], which is published in support of [2], addresses the INFOSEC activities in the system life cycle, security principles, and the INFOSEC responsibilities. The Primary Directive on INFOSEC is supported by directives addressing INFOSEC management (including security risk management, security approval, security-related documentation, and security review/inspection) and INFOSEC technical and implementation aspects (including computer and local area network (LAN) security, interconnection of CIS security, cryptographic security, transmission security, and emission security). The Primary Directive on INFOSEC itself is classified NATO Restricted and can not be discussed in this article.

The interconnection of communications and information systems is also an important part of INFOSEC [5]. “The increased number of users of interconnected CISs leads to a higher risk of unauthorised disclosure, modification or deletion of information either deliberate or accidental and of denial of service by threatening the availability of some or all CISs and/or the interconnection.” The interconnection of classified CISs should be strictly based on operational requirements and apply a restrictive policy. The security boundary as a mutually agreed physical interconnection point where the first CIS’s responsibility for the interconnection ends and where the responsibility of the other CIS starts shall be defined in the System Interconnection Security Requirement Statement (SISRS) [6].

Utilization of NATO INFOSEC policy is mandatory whenever the NATO CIS or its node is deployed within national conditions. Utilization of NATO INFOSEC policy is recommended and very useful in many other cases in the Czech Republic because of a quite poor set of CZ INFOSEC documents. In addition the usage of NATO INFOSEC policy and the documents on INFOSEC Architecture contributes to compatibility and interoperability.

NATO INFOSEC policy is applicable not only to the Ministry of Defence (MoD) but even to the Ministry of Foreign Affairs (MFA) and other organizations, whose CISs should be connected to a CIS of the European Union (EU). The Security Arrangements for the Release of NATO Classified Information to the Western European Union (WEU) (see [3]) sets out the policy, procedures and regulations required for the release of NATO classified information to WEU, and regulations for the handling of NATO classified information released to WEU. “All NATO classified information that is released to WEU is for official use only. It will, therefore, only be disseminated to individuals in WEU on a Need-To-Know basis and in accordance with stipulated release caveats. Within WEU, NATO classified information will be handled in accordance with WEU security regulations, which are based on NATO regulations.” Besides, the NATO Information Management Policy states that NATO Unclassified information is only for official use and should be appropriately protected.

3 Current state of CISs within some Czech government organizations

Some government organizations currently have a large deployed base of problem-oriented CISs. Typically, each of these has been developed by a separate service (e.g. logistic, personnel, financial) for its own use and then entered into a competition to meet the specific organization requirements. As a result, the organizations have an array of CISs that, with few exceptions, do not interoperate. There are several underlying technical reasons for this:

- CISs have been designed to different communication and IT standards and are not interoperable with other organizations’ CISs;
- In general terms, CISs have been designed to meet one specific CIS requirement and not to be sufficiently flexible to be used in other scenarios;
- The main focus of CIS security developers has been on information protection at its specific classification level, which has entailed the very rigid implementation of algorithms and other security enforcing functions (which have been heavily reliant on hardware), exacerbating still further the inflexibility problem;
- Discrete CISs have often made use of different confidentiality algorithms. This is one of the biggest problems that an organization needs to overcome if it is to develop an integrated CIS of the entire organization.
Disintegrated and non-interconnected CISs within the organization lead to serious problems, such as:

- Difficulty in systems integration in connection with overly broad diversity of technology;
- Multiplicity of databases, mail and other common services;
- High project investment needs and their low efficiency;
- High operation and maintenance requirements, lack of IT specialists;
- High requirements on communication infrastructure (too many LANs and security boundaries);
- Failure to meet user requirements on the operability and information availability from a single workstation;
- Failure to meet security requirements necessary for issue of “Approval to Operate” classified information (within the Czech condition this means the issuing of a certificate by NSA, and accreditation by the Security Authority of the given organization);
- Inability to fulfill security requirements simultaneously in all sites (nodes) of particular CISs causes the failure of certification of entire CISs and leads to operation limited to unclassified information;
- The serious problems arise when only certain sites of a particular CIS have met security requirements and should be approved to handle classified information. The main problem lies in the constitution of secure interconnection of both system parts (approved and non-approved to handle classified information), because of a lack of certified boundary protection technology. As a result the users of one part cannot reach data and services in another part (e.g. mail between the two parts).

![Diagram showing user access fails from one computer in a disintegrated infrastructure.](image)

These CISs have not yet met all of the security requirements. As a result the CIS certifications have been done either for local handling of classified information limited to a few sites, or have even failed completely and the systems handle only unclassified information. In both cases the CISs have not met the proposed network functionality and top-management, together with certain other users, have to have more than one computer to satisfy their operational requirements to access different applications of CISs. In addition there is usually no
authority that would have enough courage to decide on prompt controlled simplifying of such complicated architecture.

The complex of NATO INFOSEC measures and CIS INFOSEC Architecture compliance should be implemented into CISs. But in addition to disadvantages mentioned above, the detailed NATO INFOSEC documents are mostly classified and only in English, which is often a problem due to their quantity.

### 4 Possible way leading to integration of CISs

The analysis of the current state of non-interoperating CISs with ensuing design of the “INFOSEC Architecture of the Target CIS” should be the first step. The design should accept the layered “NATO INFOSEC Architecture” that consists of “Core Services” as an overarching computing base covering the entire organization, and “Functional Applications” as a higher level.

The second step should be projection of a “Migration Plan” from the current state to the architecture of the “Target CIS”. The migration plan should take into account the following requirements:

1. Definition of the Community Security Requirement Statement (CSRS) [6], which states the classification level, security mode of operation, management, security environment, interconnection with other CISs, and other requirements of common security policy. The common technical and architectural standards should be developed and maintained. In the case of military CISs the NATO INFOSEC architectural requirements will have been met.

2. All CISs that migrate into the common network of the future “Target CIS” should accept and implement CSRS requirements and subordinate to common management.

3. As a first phase the migration of CIS into the common network usually does not imply serious changes of technology and the CIS will more or less be operated nearly as before, but within a secure environment.

![Diagram](image)

**Figure 2:** The CISs integrated within the frame of CSRS.

4. As the second phase, the evolution-based development of CIS technology should be implemented, in which services and application would be gradually subordinated to the common standards of the integrated “Target CIS”. The core capabilities are developed as a process relatively independent of development of “Functional Applications”. The common standards should be defined and invoked.
5. The “Functional Applications” are developed independently as problem-oriented services to supersede the functionality of old CISs, and/or satisfy newly identified operational requirements of the given organization.

![Diagram of integrated IT and services within the Target INFOSEC Architecture]

The process described above is a massive intervention into CISs architecture, but should be done promptly, supported and controlled by top-level operational and security authorities.

5 Policy, classification level, and security mode of operation

The operational requirements of government organizations (especially those that have to be connected to NATO or EU classified CISs) encompass handling classified information of different levels. But the higher classified information should be protected by higher (more expensive) security measures, and the user access should be minimized.

The good Commercial Off-The-Shelf (COTS) IT products generally provide for such a level of protection that is appropriate for a non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The CISs based on such COTS IT cannot be operated in an environment in which protection is required against determined attempts by hostile and well-funded attackers to breach the system security.

The limitations mentioned above imply CISs’ separation based on the security mode of operation at the given classification level. The security principle “Need-To-Know” in this case requires using a “System-High” security mode of operation. Whenever the organization uses more than one classification level and the users do not have clearance for all classification levels, the CISs’ separation should be taken into consideration. The general concept is to operate one relatively broad CIS for Restricted information, and, where applicable, to develop a CIS for a Confidential and/or Secret level for those users who have personnel clearance and “Need-To-Know” to handle such a level of classified information.

Where the organization develops CISs for different classification levels, the architecture, standards, services, and applications may be the same for all CISs in order to save on investment. The appropriate security measures corresponding to the CIS security level should be satisfied by a secured environment and communication security measures. All components and services on the boundary between two CISs should be developed in...
compliance with accepted standards and coordinated with the appropriate authority of the interconnected CISs to reach interoperability and consistency of security measures. Both operational and security requirements should be defined in advance for boundaries between such CISs.

![Diagram of interconnection of government organization CISs]

Figure 4: The model situation of interconnection of government organization CISs.

The Directive for the Interconnection of Communications and Information Systems [5] should be invoked when the boundary protection services are designed, implemented, and documented. The directive sets out security principles and minimum-security requirements for different scenarios of interconnected CISs based on mission, classification level, and level of trust between the two sides.

All security aspects of interconnection of two CISs should be described in the document “System Interconnection Security Requirement Statement” (SISRS) [6] and boundary protection devices should be operated under conditions stated in the “Security Operational Procedures for Interconnection of CISs”. The security authorities of both CISs should approve their respective interconnection measures before the start of operation.

Figure 4 above shows various scenarios of CIS interconnection. The establishment of a boundary should be based on the “Security Agreement” between the government organizations to be interconnected, and in compliance with the directive [5]. The level of trust between those organizations, classification level of CISs, permitted data flows and other aspects should be taken into account for definition of boundary functionality and EAL (Evaluation Assurance Level, see [8] and [5]). Where the level of risk is too high or where there is a lack of sufficient technology, the air gap or one-way data flow technology should be implemented to fulfill operational requirements.

6 Conclusions

The Czech national CISs that handle classified information should invoke Czech Act No 148/1998 Coll. on “Security of Classified Information” [1] and supporting directives of CZ NSA. The detailed security principles, minimum standards, life cycle requirements, risk evaluation and vulnerability reports, risk management
procedures etc., that are stated in Directives of NATO Security Policy, should be used and implemented, where applicable.

The layered “NATO INFOSEC Architecture” with “Core Services” and “Functional Applications” should be accepted in order to reach high efficiency. The system core should be designed as an overarching computing base covering the entire organization, relatively stable, with evolution-based development. The “Functional Applications” should be flexible to changing organization needs.

The acceptance and implementation of “NATO INFOSEC Architecture” is necessary in order to reach interoperability of Czech national CISs with NATO CISs.

The interconnection of two CISs must be strictly based on operational requirements and invoke the appropriate NATO INFOSEC Directive. Where the risk arising from interconnection is too high, the boundary protection devices should be alternatively based on one-way security mechanisms excluding network services connectivity.

The operational and security authorities should undertake responsibility and actively govern the migration of current separated and non-interoperating CISs toward integration.

References