REGULATION
on Protection of Confidential Information, Security Clearances and Security Approvals in the Field of Security and Defence

CHAPTER I
General provisions
Article 1
Objective

The objective of the present Regulation is:

a) to protect documentation, cf. Article 2, from unauthorised access, the prevention of which is imperative, provided it contains information relating to State security, defence issues, or external relations with other States or transnational organisations, i.e. information the secrecy of which is primarily in the interest of the public;

b) to fulfil obligations in accordance with international agreements concerning security and defence, which provide for confidentiality and safekeeping of specified information and documentation;

c) to secure appropriate handling and security of such documentation, irrespective of its origin; and

d) to lay down rules on company security clearance for companies which are in need of such clearance on account of their export interests.

Article 2
Scope of application

This Regulation shall apply to:

a) confidential information, covered by the Defence Act No 34/2008, including its security and handling;

b) security clearance and security approval for individuals, companies, including suppliers, service providers and exporters, organisations, communication information systems (CIS), equipment and installations within the field of security and defence, covered by the Defence Act;

c) access to confidential information, security clearances and security approvals based on the Agreement between Iceland and the European Union on Security Procedures for the Exchange of Classified Information of 12 June 2006 and its annex, Security Arrangements between the Ministry for Foreign Affairs (MFA) of the Republic of Iceland, the EU Council General Secretariat Security Office (GSCSO) and the European Commission Security Directorate (ECSD) for the Protection of Classified Information Exchanged between The Republic of Iceland and the EU;

d) access to confidential information, security clearances and security approvals based on the General Security Agreement on the Mutual Protection and Exchange of Classified Information between Denmark, Finland, Iceland, Norway and Sweden of 7 May 2012;

and

e) access to confidential information, security clearances and security approvals based on other international agreements to which Iceland is a party.

Article 3
Definitions

For the purpose of this Regulation:

a) 1. the term "**Authorisation for Access**" means: a decision taken by the director of an organisation or a company that an individual is authorised to have access to secure areas or information with a distinctive security marking, provided he/she has been given security clearance;

b) 2. the term "**Background Check**" means: an examination undertaken by the National Security Authority (NSA) of the identity of the individual concerned and of police documents, *inter alia* his/her record of convictions, including if he/she has a criminal record, as part of assessing whether it would be safe to issue a security clearance for that individual and hence authorise his/her access to sensitive areas and confidential information;

c) 3. the term "**Supplier**" means: a person or entity selling goods which relate to the handling of confidential information and are covered by the present Regulation;

d) 4. the term "**Courier Certificate**" means: a confirmation issued by an organisation that a delivery, comprising confidential information, is authorised and that the individual carrying the information does so under the authority of the Government;

e) 5. the term "**Company**" means: a legal person, including suppliers, service providers or exporters, involved in handling of confidential information covered by the present Regulation;

f) 6. the term "**Procuring Entity**" means: an administrative body purchasing goods or services from a legal person outside the Government;

g) 7. the term "**Administrative Area**" means: an access controlled area which has passed inspection by NSA and has been authorised to handle confidential information up to the security marking "*Restricted*" (incl.), in accordance with this Regulation, cf. Articles 5 and 7;

h) 8. the term "**Document**" means: data of any kind comprising information, written or in other form, that have been created, received or maintained while an organisation or an individual engages in its/his/her activities;

i) 9. the term "**Organisation**" means: an administrative body to which this Regulation applies;

j) 10. the term "**Classified Information**" means: confidential information with a distinctive security marking and where access to such information is controlled with relation to security markings, security clearances and/or security approvals and with relation to those who need to have access to it;

k) 11. the term "**Classified Data**" means: the physical form in which confidential information is stored;

l) 12. the term "**Security Marking**" means: classification and marking of confidential information with regard to the seriousness of unauthorised access;

m) 13. the term "**Registry**" means: an archive of confidential documents, where reception, registration, distribution, placing and destruction of confidential information takes place within the organisation or company concerned;

n) 14. the term "**Confidential Information**" means: information covered by the present Regulation, the confidentiality of which is of vital interest;

o) 15. the term "**Information**" means: information of any kind, irrespective of its form, including documents (in electronic or paper form), such as maps, photographs or video and audio recordings, or other data;

p) 16. the term "**Security Officer**" means: officer of an organisation or a company entrusted by its director with the task of implementing this Regulation;

q) 17. the term "**Service Provider**" means: a party that provides services relevant to the handling of confidential information in accordance with the present Regulation;

r) 18. the term "**Secure Communication Information System (CIS)**" means: organised combination of peripheral equipment, software, data systems and communications network, all of which are encrypted in the appropriate manner and have been security approved in accordance with the present Regulation;

s) 19. the term "**Security Competence**" means: competence of an individual, organisation, company, area or equipment to receive security clearance and/or security approval for a distinctive security marking;

t) 20. the term "**Security Agreement**" means: agreement between an administrative body and a supplier, service provider or an exporter concluded, concurrent with classified procurement of goods or services or with classified export, before access is granted to confidential information;

u) 21. the term "**National Security Authority (NSA)**" means: central organisation which, on behalf of the State, coordinates and oversees handling and safekeeping of confidential information, runs background checks and determines security clearance and/or security approval for individuals, organisations, companies, areas, communication information systems (CIS) and equipment on a domestic level and vis-à-vis foreign countries and international organisations, cf. also Article 4(1);

v) 22. the term "**Secure Area**" means: an access controlled area which has passed inspection made by NSA and where it is authorised to handle confidential information with the security marking "C*onfidential*" and above, in accordance with this Regulation;

w) 23. the term "**Inspection**" means: NSA's surveillance of organisations, companies, areas, facilities and/or buildings, communication information systems (CIS) and equipment, which have been security cleared and/or security approved, and surveillance of implementation of the present Regulation;

x) 24. the term "**Personnel Security Clearance**" means: NSA's attestation based on a background check on an individual's security competence for having access to confidential information up to a distinctive security marking;

y) 25. the term "**Company Security Clearance**" means: NSA's attestation, based on background checks on individuals (chairmen of the Board of Directors and/or employees), and, as appropriate, inspection made on the facilities of a company and on its competence for engagement in activities or research which require access to confidential information;

z) 26. the term "**Security Approval of CIS**" means: NSA's attestation of the fact that a system or equipment, in which confidential information is placed or handled or to which and/or from which such information is communicated, meets the appropriate security requirements;

27. the term "**Security Approval of Facilities**" means: NSA's attestation, based on inspection made to determine whether a certain space, area or facility, within an organisation or a company, meets the appropriate requirements applicable to administrative areas and secure areas I or II for storing confidential information up to a distinctive security marking, cf. Articles 5 and 7;

28. the term "**Classified Procurement**" means: a procuring entity's procurement, the nature of which requires suppliers or service providers to have access to confidential

information, equipment or objects, or requires that they need to be security cleared for other reasons;

Article 4
Responsibility and Surveillance

The National Commissioner of the Icelandic Police (NCIP) performs the role of NSA, as defined in this Regulation, subject to the international organisations' rules with relevance to the present Regulation.

The director of an organisation or the manager of a company, which has received security clearance or has security cleared employees in its services, is responsible for implementation of this Regulation within the said organisation or company. He or she shall:

(a) himself or herself be security cleared in accordance with this Regulation;
(b) entrust one of his or her employees to be security cleared in accordance with this Regulation and to perform the role of security officer;
(c) ensure that the employees of the organisation or the company, who need access to classified information in accordance with this Regulation, will be security cleared as the Regulation stipulates;
(d) ensure that the rules of procedure of the organisation or the company are in line with this Regulation;
(e) compile internal instructions for the handling of classified information and security instructions, based on the provisions of this Regulation, elaborated in more detail as may be required;
(f) brief his or her employees regularly on this Regulation, the rules of procedure of the organisation or company in question, internal security instructions and on more detailed elaboration thereof; and
(g) secure the operation of a registry within the organisation or the company, where relevant.

In case of suspicion of a breach of the present Regulation, this shall be notified without delay to the security officer, the director of the organisation and the manager of the company concerned, and the NCIP. If a breach is confirmed, this shall be notified to the security officer of the Ministry for Foreign Affairs.

The NCIP shall inspect organisations, companies, areas, communication information systems (CIS) and equipment, which the NCIP has security cleared or security approved, cf. Article 37.

CHAPTER II
Classification, Storage, Handling and Communication of Classified Information
Article 5
Classification

Classified information shall be used exclusively for the purpose specified and shall be handled in line with its classification, as provided for in this Article.

Classified information may be handed over only to individuals who, in the course of their work, need access to the information and have been security cleared for that purpose in accordance with this Regulation.

Confidential information shall be classified according to a distinct security marking, which shall be clearly designated. Classification of confidential information with distinct security markings is based on estimation of the damage that could result from unauthorised release thereof. Confidential data shall be classified and marked with one of the following security markings; from the highest (a) to the lowest (d):

a) (a) ALGJÖRT LEYNDARMÁL (“YDERST HEMMELIGT”, “COSMIC TOP SECRET”, “TRÈS SECRET UE” or equivalent) shall be used in cases when the security

of Iceland, other States or international organisations, relations with foreign Governments or international organisations, or other vital interests of the State may suffer deadly serious damage by unauthorised release thereof;

b) (b) LEYNDARMÁL ("HEMMELIGT", "NATO SECRET", "SECRET UE" or equivalent) shall be used in cases when the security of Iceland, other States or international organisations, relations with foreign Governments or international organisations, or other vital interests of the State may be seriously damaged by unauthorised release thereof;

c) (c) TRÚNAÐARMÁL ("FORTROLIGT", "NATO CONFIDENTIAL", "CONFIDENTIEL UE" or equivalent) shall be used in cases when the security of Iceland, other States or international organisations, relations with foreign Governments or international organisations, or other vital interests of the State may be damaged by unauthorised release thereof; and

d) (d) TAKMARKAÐUR AÐGANGUR ("TIL TJENESTEBRUG", "NATO RESTRICTED", "RESTREINT UE" or equivalent) shall be used in cases when it may be contrary to the interests of Iceland, of other States or international organisations, or may have adverse effects on relations with foreign Governments or international organisations, if the information is released to unauthorised parties.

Data marked "NATO UNCLASSIFIED" are the property of the North Atlantic Treaty Organisation, whereas their release is subject to NATO regulations.

The originator of classified data shall ensure that they have appropriate security marking. Classified data shall not have higher security marking than is necessary. The period of validity for a security marking according to this Article shall not be longer than is necessary. Icelandic classified data to be communicated abroad shall be marked "ISL" plus the appropriate security marking (e.g. *"ISL Restricted"*), unless international agreements state otherwise.

Article 6
Handling of Classified Information

Classified information shall be handled as follows:

a) the information shall be protected and kept safe in a secure manner;

b) where the information is used in new data, the data shall have the same security marking as the document of origin;

c) should the information be copied or translated, the document shall have the same security marking as the document of origin; A translation of such confidential document shall include a detail specifying that the document contains classified information from the State or organisation of origin,

d) where information with the security marking "C*osmic Top Secret*" is no longer needed, it shall be given long-term physical protection, cf. Article 13, it shall be destroyed, cf. Article 12, or it shall be returned to the state or organisation of origin, as appropriate. Documents with the security marking "*Secret*" or below shall be destroyed as provided for in this Regulation; and

e) if a crisis situation makes it impossible to protect classified information, the information shall be destroyed.

Furthermore, it is unauthorised, without a prior written authorization from the State or organisation by which the information is originated:

a) to change the security marking of a document;

b) to translate, copy or destroy documents with the security marking "C*osmic Top Secret*";

c) to release classified information to other States, organisations or unauthorized parties, except with explicit authorisation and when this is strictly necessary; and

d) to transfer classified information out of the country, except with explicit authorisation and when this is strictly necessary.

Article 7
Storage of Classified Information

Classified information shall be stored in secure storage places, a certified information system, or in areas, provided for the purpose, where distinctive rules of conduct apply and where special security device has been put in place. The said areas are of three categories:

a) Secure Area I;
b) Secure Area II; and
c) Administrative Area.

Secure Area I and Secure Area II are especially defined and access controlled areas. The said two areas shall be equipped with a burglar-alarm system equipped with electronic detectors connected to a security centre. Secure Area I is monitored 24 hours a day and only security classified individuals have authorised access thereto, except the security officer concerned decides otherwise. Secure Area I and Secure Area II may be unified, where exceptional circumstances justify this and provided the classified information is not compromised.

Classified information with security marking:

a) "*Cosmic Top Secret*" shall be stored in Secure Area I;
b) "*Secret*" and "*Confidential*" shall be stored in Secure Area I or II; and
c) "*Restricted*" shall be stored in Secure Area I or II or in Administrative Areas, provided the information is stored in locked storage places or in locked offices in the Administrative Area.

On leaving his/her office or workspace, an individual, in possession of classified information, shall ensure that the information is stored in authorised and locked storage places in Secure Areas, cf. paragraph 1, and in accordance with its security marking.

Article 8
Release of Classified Information

The Ministry for Foreign Affairs is responsible for the release of classified information on domestic territory, i.e. information received from abroad on the basis of international agreements, unless specific provisions stipulate otherwise. Before the said classified information is released, a security clearance and/or a security approval shall have been issued for:

a) the individual concerned, who is to receive the information, stating that he/she satisfies the conditions for access to classified information;
b) the company or organisation concerned, which is to receive the information, stating that it has acceptable facilities, if applicable, for storing classified information and for controlling access thereto; and
c) equipment, such as information systems, in or from which the information shall be stored or released, stating that the equipment is satisfactory with regard to the security of information, if appropriate.

Article 9
Security, Marking and Transfer of Classified Information

The security of classified information shall be ensured during its life-cycle.

Classified information marked "*Confidential*" and above shall be included in a register where its reception, handling, distribution and destruction is entered.

When classified information is transferred from one place to another, it shall be wrapped in opaque double transport packaging or envelops. The inner packaging shall be sealed and

labelled with the appropriate security marking and with the names of the receiver and the originator. The outer packaging shall be sealed and marked exclusively with the names of receiver and originator. Thus, classified information marked "*Restricted*" may be sent by conventional post.

Classified information marked "*Confidential*" and above shall be transferred from one place to another in the keeping of a security cleared individual, who shall have knowledge of any rules applicable to the transfer of classified information.

When classified information marked "*Confidential*" and above is transferred from one State to another, the security cleared individual, who makes the transfer, shall be in possession of formal courier certificates, as a confirmation, issued by the organisation of origin. A courier certificate shall explain from where and to which destination the delivery shall be transferred, the courier's travel plan, and the reference number in the delivery. Classified information transferred from one State to another shall be exempt from customs searches, when border check is conducted, provided the courier has the above mentioned courier certificate in his/her possession.

Article 10
Re-assessment and Period of Validity of Classified Information

The security markings of classified information shall be re-assessed regularly or at least every five years. In principle, confidential documents marked "C*osmic Top Secret*" shall be declassified after 30 years, marked "*Secret*" after 15 years, and marked "*Confidential*" after 5 years.

Article 11
Computer Security

It is forbidden to convert classified information, under the scope of application of the present Regulation, into electronic form, or transfer such information by electronic means, except via approved information systems, cf. Article 22. The said classified information may not be transferred by conventional electronic mail.

Security cleared individuals shall, in their absence, shut down their computers, in which classified information is stored. They may never release their user name and/or password to any one.

An organisation or a company, which has in place a security approved information system, shall regulate controlled access to classified information stored therein, in order to ensure that individuals, who have access to the information, have received adequate security clearance as laid down in this Regulation and by other applicable rules within which the information may fall.

Article 12
Reproduction of Confidential Documents, Destruction and Declassification

Confidential documents may only be photocopied in approved photocopying apparatus, which is not computer connected, and ink cartridges shall be destroyed according to rules applicable to classified information.

Where a document, security marked "*Confidential*" or above, is reproduced, the number of copies shall be recorded, together with the names of the recipients. Only necessary number of copies shall be made.

Copies of confidential documents shall be destroyed after use, in a paper shredding machine or by burning them.

Should security markings be degraded or relieved, the document's security classification shall be crossed out and the date of adjustment and initials of the person responsible entered,

cf. also Article 6. Furthermore, the adjustment shall be included in the register of classified information.

Article 13
Registry and Depository Body

An organisation or a company, where classified information is handled by its employees in accordance with the present Regulation, shall operate a special Registry, where it is guaranteed that the information is handled in accordance with the present Regulation. The registry shall keep a register of classified information during its life-cycle from its establishment or reception until it is put in durable storage or destroyed. Each organisation or company shall register the reception, handling, the person responsible, distribution, placing and destruction of classified data. Access to the registry shall be restricted.

Registries shall be situated in a secure area, cf. Article 7, and its registrar shall be security cleared up to the highest security marking of documents stored in there, or up to the security marking consistent with the security clearance of the company in question. A registry shall be kept separate from the general archive of an organisation or a company. Registries shall be subject to inspection made by the NCIP every two years. Organisations and companies shall adopt safekeeping policy and rules of procedure with respect to the operation of their registries.

When there is no longer any need for the classified information, it shall be submitted to a special secure archive of the Minister for Defence Affairs, or be destroyed in accordance with the present Regulation.

Any requests for access to classified information shall be submitted to its originator, as its labelling specifies.

CHAPTER III
Authorisation for Access
Article 14
Grant of Authorisation for Access

The director of an organisation or the manager of a company is responsible for granting an individual authorisation for access, i.e. an individual whose duties require access to classified information in accordance with the provisions of this Regulation.

It is forbidden to grant anyone authorisation for access to classified information, areas, quarters, constructions, equipment or security agreements without prior confirmation, issued by the NCIP, that the individual concerned has received appropriate security clearance.

In cases where it is strictly necessary, e.g. when overriding reasons relating to public interest require so, an authorisation for access may be granted to an individual, notwithstanding he/she has not received security clearance from the NCIP, provided the security of classified information is not compromised. The NCIP shall be notified forthwith of such exemptions, should they be granted.

Article 15
Access to Classified Information

Before classified information, with the security marking "*Confidential*" or above, is handed over to an individual, he/she shall have received appropriate security clearance in accordance with the present Regulation. Personnel security clearance shall be determined for a specific security marking which shall not be higher than strictly necessary.

Data with the security marking "*Confidential*" or above shall be handled exclusively by parties that are security cleared for that marking or above.

Even though a personnel security clearance will grant access to specific data, access shall be limited to those data that are absolutely necessary.

Article 16
Access to Areas

Before an individual is granted access to areas, where classified information is stored or handled, he/she shall have received appropriate security clearance, in accordance with the present Regulation, and if not, special security measures must have been taken in order to conceal the information and further still, the individual concerned shall be escorted by a security cleared individual. Otherwise, the director of an organisation or the security officer concerned shall grant authorisation for access to such areas.

The names of guests invited by an organisation, who gain access to a storing place for classified information or to places where such information is handled, shall be taken down, together with the time of their arrival and departure. They shall always be escorted by a security cleared individual.

A security officer may grant employees of an organisation, who have not received security clearance, access to a storing place for classified information, e.g. for maintenance or cleaning purposes, provided appropriate measures have been taken to conceal the information or to ensure that the said employees are, at all times, escorted by a security cleared individual.

Article 17
Withdrawal of Authorisation for Access

Authorisations for access shall expire when:

a) an individual terminates his/her employment for which the authorisation was required;
b) there is, for other reasons, no longer need for an authorisation; or
c) the individual concerned is no longer in possession of a valid security clearance in accordance with this Regulation.

Where information emerges, from which security competence of a security cleared individual may be doubted, the director of an organisation or the manager of the company concerned shall withdraw the authorisation for access or restrict or suspend it. Such decision shall be notified the NCIP who shall determine whether the individual's security clearance shall remain unchanged.

Should the NCIP withdraw security clearances, cf. Article 28, authorisations for access of the individuals concerned shall also be withdrawn in accordance with this Article.

Decisions of the directors of organisations or managers of companies are final.

Article 18
Access of Head of State and Ministers of Government

Access to classified information may be granted to the President of Iceland and Ministers of the Government of Iceland who have not received security clearance in accordance with the present Regulation. Before such access is granted, they shall be made aware of their obligations concerning confidentiality and their responsibilities when the handle classified information in accordance with the present Regulation. The before mentioned parties shall maintain strict confidentiality of information which they receive on the basis of this permit.

CHAPTER IV
Security Clearance and Security Approval
Article 19
General Provisions on Security Clearance and Security Approval

The Minister for Defence Affairs is responsible for the issue of security clearances and security approvals in accordance with the present Regulation. The NCIP shall issue security clearances and security approvals in accordance with the present Regulation, acting in the name of the Minister for Defence Affairs.

Article 20
Personnel Security Clearance

Before an individual receives security clearance he/she shall have passed background check, signed a solemn declaration concerning the maintenance of confidentiality with regard to confidential information to which he/she receives access in the conduct of his/her official duties, and have been briefed by the NCIP on rules applicable to handling of classified information. Confidentiality shall be maintained, even if a position is relinquished or an assignment completed.

Background checks, run by authorities in another State, shall be approved in Iceland, on request and if substantiated by appropriate documentation. When establishing security clearance in such cases, the background check, run by NSA in the home State of the individual in question, shall be subjected to scrutiny.

The NCIP may decide to run a background check on an individual, before he/she receives security clearance according to this Regulation, even though the said individual has been subjected to such a check in another State.

Each organisation or company, that has security cleared individuals as their employees, shall keep an updated register of the said employees. The following shall be registered: the period of validity of security clearances, security markings, and whether the clearance has expired, has been withdrawn, has been suspended or is being processed.

Security officers have a responsibility to ensure that employees have, at all times, required valid security clearance up to the appropriate security marking.

Article 21
Company Security Clearance

Companies, including suppliers, service providers, parties seeking tenders, contractors, or exporters, where employees have access to classified information or facilities, where classified information is stored or handled, shall be security approved. Thus, members of the Board of Directors and managers of such companies shall, together with their security officer, pass security clearance, cf. Article 20.

The issue of security clearance for a company shall be based on a request from a procuring entity (buyer) purchasing goods or services from the company (seller). A procuring entity's application for a company security clearance shall be submitted in a form designed for that purpose and developed by the NCIP. Furthermore, a security agreement shall have been concluded between the procuring entity and company concerned, cf. Article 25. A procuring entity may submit a request for a new company security clearance and/or for the upgrading of the security marking of the company's security clearance which the company has already received.

Before an employee of a company gains access to classified information up to the security marking "*Confidential*" (incl.) or above, or if this is otherwise considered necessary, he/she shall be security cleared up to the appropriate security marking.

A security clearance shall not be issued for a company, if reasonable doubts arise about the security competence of the company or its employees. Relations concerning the competence of the company or its employees shall be assessed exclusively, and their will to implement preventive security measures as provided for in this Regulation. In making the said

assessment a background check shall be run on the members of the Board of Directors and managers of the company in accordance with Article 30, cf. Articles 31 and 32.

Companies shall provide all information necessary for the assessment of their security competence, and that of their employees, for the purpose of determining security clearances.

Head of a companies shall, without delay, inform the NCIP of:

a) any alterations in the appointments of the members of their Boards of Directors and/or of their managers;
b) transfer of ownership, in the company concerned, to new parties;
c) any transfer of activities or equipment;
d) any changes made to quarters, facilities or equipment which have been security approved earlier;
e) any authorisations granted to the company for moratorium, to seek composition or composition with creditors, or of insolvency proceedings concerning the company; or
f) of any other issues that may effect the security competence of the company concemed according to the present Regulation.

When circumstances arise within a company that might compromise security according to this Regulation, and no preventive security measures can diminish the compromise, the NCIP may withdraw the company's security clearance in accordance with the provisions of Article 28.

Classified information or equipment, in which such information is stored, may not be transferred to new owners of a company, unless the new owner has been security cleared in accordance with this Regulation. The equipment may still be transferred to new owners, provided all classified information has been deleted from the equipment in accordance with this Regulation.

The Minister may conclude security agreements with Icelandic parties (exporters) in need of security clearance for the purpose of engaging in international trade. The provisions of this Article and of Article 25 shall apply to such agreements *mutatis mutandis*.

A security clearance may not be issued for a company, including suppliers, service providers, contractors, or exporters, unless its employees, who are to handle classified information in accordance with this Regulation, have passed background checks pursuant to Article 30, cf. Articles 31 and 32, and, where applicable, the company's facilities meet the conditions of Articles 7 and 23.

Article 22
Security Approval of Information Systems and Equipment

Before classified information is handled, stored or released in a secure information system, the NCIP shall approve the system up to the appropriate security marking.

The NCIP may entrust other parties, that have received appropriate clearance, with the task of performing security service for information systems in which classified information is handled.

The NCIP shall approve equipment, tools and procedures for the destruction of classified information, cf. Article 12.

Security approvals may not be issued for information systems or equipment, unless they meet the safety standards and requirements of the information system involved.

Article 23
Security Approval of Facilities

The NCIP shall issue security approvals for quarters, areas and facilities for the benefit of those who handle classified information and keep such information safe. The said quarters,

areas and facilities shall satisfy the conditions for minimum security and shall pass security approval, cf. Article 7.

Article 24
Duration of Validity of Security Clearances and Security Approvals

The period of validity of a security clearance for an individual shall be as follows:

a) one year in case of initial security clearance;
b) two to five years, as determined by the NCIP, in case of a renewal; or
c) five years in case of a renewal of security clearance for a public servant, employed on a permanent basis, who handles classified information regularly.

The period of validity of a security clearance for a company shall be as follows:

a) two years in case of initial security clearance; or
b) three to five years, as determined by the NCIP, in case of a renewal.

Period of validity of a security clearance, different from that stipulated in paragraph (a) and (b) and compatible with the period of validity of a security agreement, may be determined.

The period of validity of security approvals for information systems and equipment shall be as follows:

a) of an interim approval to operate (IATO), maximum twelve months; or
b) of a security approval, maximum three years.

The period of validity of security approvals for facilities shall be three years, unless adjustments are made of such approvals. Organisations may still be granted security approvals for facilities for a longer period and even of unlimited duration, as the case may be, on special grounds.

The period of validity of security clearances and/or security approvals shall be clearly indicated at the time of their issue.

A security clearance shall expire when:

a) its period of validity comes to an end;
b) a security agreement, cf. Article 25, expires or the period of validity of the project in question comes to an end;
c) an individual, for whom a security clearance was required, terminates his/her employment;
d) the company in question is the subject of a declaration of bankruptcy or terminates its business activities; or
e) the need or prerequisites for a security clearance cease to exist on other grounds.

A security approval shall expire when:

a) its period of validity comes to an end;
b) information systems or equipment no longer meet the requirements of this Regulation;
c) the facilities of the company or organisation concerned have been altered or they no longer meet the requirements of this Regulation;
d) the company, where the equipment is kept, becomes the subject of a declaration of bankruptcy or terminates its business activities; or
e) the need for a security approval ceases to exist on other grounds.

Article 25
Security Agreements

An organisation, which stores classified information in accordance with the present Regulation, shall enter into security agreements with those suppliers and service providers that, on account of the transactions implicated, need access to the said information. Such agreements are the basis for the NCIP's company security clearances, cf. Article 21, up to the appropriate security marking, if applicable.

The NCIP may decide that security agreements, cf. paragraph 1, should be concluded, if suppliers or service providers should need access to security cleared computer systems or storing places, or if security agreements are considered necessary for other reasons. Security agreements shall be concluded before suppliers or service providers are granted access to classified information.

Security agreements, in the form of an annex to a work contract concerning security classified purchase of goods or services or an invitation to tender, shall provide for responsibilities and obligations in accordance with the present Regulation, including with regard to:

a) the security markings of the transactions, specially indicated for each part of the work;
b) the running of background checks on suppliers or service providers and the conduct of other inspections, the purpose of which is to assess safety factors and whether suppliers or service providers give effect to the security provisions of the contract and meet other obligations in accordance with the present Regulation;
c) the period of validity of security agreements, if applicable; and
d) the consequences of breaches of security agreements, including contractual fines.

Expenses or requirements undertaken or reimbursed or fulfilled by suppliers or service providers, when they comply with the provisions of this Regulation or provisions related thereto and adopted by way of concluding security agreements, are beyond the control of the procuring entity or the NCIP, unless expressly indicated to the contrary in the security agreements.

Article 26
Refusal to issue a Personnel Security Clearance

An individual, for whom a security clearance has been requested, shall, in accordance with Article 30, cf. Articles 31 and 32, be notified of the results of the background check as soon as possible. An individual, who, in the opinion of the NCIP, does not meet applicable assessment criteria in determining his/her security clearance in accordance with Articles 31 and 32, shall not receive security clearance.

Refusal of security clearance shall be subject to the rules of procedure of the Administrative Procedures Act. Should the NCIP decide to refuse to issue a security clearance for an individual on the basis of his/her background check, the NCIP shall inform the individual concerned of the intended refusal and of the reasoned justification thereof. Still the justification shall not include information, the secrecy of which is essential, whereas such information:

a) is important or may be detrimental for the security of Iceland or her associate States, relations with foreign Governments, or for other important security interests of the State;
b) is important for the protection of sources of information;
c) concern the said individual's relations with other individuals close to him/her, i.e. relations that he/she should not have knowledge of;
d) concern technical equipment, production information, business intelligence or business accounts, business secrets, or such information that others may use when they engage in their activities; or
e) concern criminal matters or law enforcement investigation to which the individual concerned is linked in some way, and can not be made public.

Before a decision on refusal of security clearance is taken, the individual concerned shall be granted the right of adversarial approach in accordance with the provisions of the Public Administration Act.

Should the NCIP decide to refuse to issue a security clearance, after the individual concerned has had the opportunity to make use of the adversarial approach, that decision shall be formally notified to the said individual and to the requestor of the background check. The NCIP's decision to refuse to issue a security clearance shall always be duly motivated, subject

to the provisions of paragraph two, in accordance with the provisions of the Public Administration Act. Nevertheless, the requestor of the background check shall only be notified of the fact that the issue of a security clearance has been refused on the basis of the present Regulation, without presenting any reasoning or further explanatory notes. The NCIP's decision shall include guidance notes on how to avail oneself of the freedom to submit an appeal to the Minister for Defence Affairs, in accordance with the provisions of the Public Administration Act.

A party to a case has the right to see any documents and other data concerning the matter at hand, in accordance with the provisions of the Public Administration Act, with such exceptions as are contained therein. Furthermore, the NCIP may, in particular cases, restrict the said party's access to data, where its interest in the exploitation of the data should be subordinated to greater public or private interest, cf. the provisions of the Public Administration Act. Such assessment shall *inter alia* take account of the points specified in paragraph two. The merits of the case shall be considered exclusively on a case-by-case basis.

Article 27
Refusal to issue a Company Security Clearance

Results of checks, according to Articles 21 through 23, cf. Article 7, shall be notified, as soon as possible, to the director of the organisation concerned or the manager of the company concerned who has requested a company security clearance. Companies or organisations, facilities, information systems or equipment shall not receive security clearances or security approvals, if, in the opinion of the NCIP, the criteria, according to Articles 21 through 23, cf. Article 7, are not met.

Where refusal of company security clearance is imminent and before a final decision is made, the rules of procedure of the Administrative Procedures Act shall be applied as concerns the parties' right to be informed of any justifications and their right of adversarial approach.

Should the NCIP determine to refuse to issue a company security clearance, this decision shall be notified to the director of the organisation concerned or the manager of the company concerned.

Article 28
Withdrawal of Security Clearances

Security officers shall, without delay, notify the NCIP of the termination of office of any individual who has received security clearance in accordance with this Regulation, or of the fact that security clearance of the individual in question is no longer needed. In that case the NCIP shall forthwith withdraw the security clearance of the said individual.

Further still, security officers shall, without delay, notify the NCIP of any altered circumstances of a company, such as changes of ownership, financial standing, quarters, areas, employees, or other things of relevance that could have effect on the company's or its employees' security competence to enjoy security clearance. The NCIP shall then determine at once if the company's security clearance should be withdrawn, and if so implement the withdrawal in accordance with the provisions of this Article, as the case may be.

When the period of validity of a security clearance expires, the NCIP shall notify the individual concerned and the security officer of the organisation or company in question of the expiration of the security clearance.

Where information emerges, that may have effect on the security competence of a security cleared individual, the NCIP shall be informed of this without delay and shall determine whether the said individual's security clearance should be suspended or withdrawn and the case examined further.

Should the NCIP decide to withdraw or suspend security clearance, this shall be notified to the individual concerned, without delay, and to the company or organisation which applied for security clearance for the said individual.

In case of withdrawal of an individual's security clearance, the rules of procedure in Article 26 shall apply. The NCIP may suspend security clearances while an appeals procedure is being followed in accordance with Article 38.

The managers of companies shall be notified of imminent withdrawals of security clearances and of the reasons thereof, and shall be given opportunity to make use of the adversarial approach in accordance with the provisions of the Public Administration Act. Final decision of the NCIP to withdraw a company's security clearance shall be duly motivated in accordance with the provisions of the Public Administration Act.

Article 29
Withdrawal of Security Approvals

Security officers shall, without delay, notify the NCIP of all alterations which have been made to an information system, equipment, facilities or space of a company or an organisation, which has received a security approval in accordance with the present Regulation, or where there is no longer need for any security approval. The NCIP shall then and without delay withdraw the said security approval, where applicable.

When the period of validity of a security approval expires, the NCIP shall notify the security officer of the organisation or company concerned thereof.

Where information emerged that may have effect on security approvals in accordance with the present Regulation, the NCIP shall be informed of this without delay and shall determine whether the said security approval should be suspended or withdrawn and the case examined further.

Should the NCIP decide to withdraw or suspend security approvals, this shall be notified, without delay, to the security officer of the organisation or company which applied for the approval.

The directors of organisations or the managers of companies shall be notified of imminent withdrawals of security approvals and of the reasons thereof, and shall be given opportunity to make use of the adversarial approach in accordance with the provisions of the Public Administration Act. Final decision of the NCIP to withdraw an organisation's or a company's security approval shall be duly motivated in accordance with the provisions of the Public Administration Act.

CHAPTER V
Background Checks

Article 30
Running of a Background Checks on Individuals

The NCIP shall run background checks on individuals at the request of the party responsible for granting access in accordance with Chapter III. The Minister shall decide which companies or organisations are competent to submit requests for security clearances in accordance with the present Regulation.

Background checks may *inter alia* include police records checks on the individual concerned, including in police case lists, checks on certificates from the police registry, on Interpol's information system, the SIS-information system, information from the civil status records; may include queries to foreign authorities, where applicable, checks of customs authorities records, district courts records and of other records.

When security clearance up to the security markings "*Confidential*" and "*Secret*" (incl.) is issued, background checks shall be run at least five years back in time. When security

clearance up to the security marking "C*osmic Top Secret*" (incl.) is issued, background checks shall be run at least ten years back in time.

Background checks shall include assessment of information provided by the individual concerned, of information maintained by the NCIP, and information from public records, where applicable, cf. paragraph two. Organisations, from which the NCIP asks for information, are obliged to release information from their records to the NCIP. Information from records shall be released in writing or electronically. Background checks may include other sources as well, e.g. information from workstations, government agencies, and from other sources, where applicable. Information gathered in the process of background checks shall be submitted to the NCIP free of charge.

Background checks shall not be made, unless the individuals concerned have been informed of the need thereof and let know from where information will be gathered, and unless the said individuals have given their formal consent in a form designed for that purpose by the NCIP. Having given their consent the individuals concerned are obliged to provide complete and correct information, *inter alia* on any relationship that may have effect on the estimation of their security competence.

The accuracy of background checks shall be directly proportional to the heightening of security markings. When running security clearance for the security marking "*Secret*" or above, or in other special cases, background checks may cover individuals with family ties with the original subjects of the check, or those who reside with them, provided the said individuals have given their prior informed consent.

Information received by the NCIP in the context of background checks shall be used exclusively for the purpose of security clearance in accordance with the present Regulation. Measures shall be taken to ensure that only employees, who run security clearances, have access to the aforementioned information.

Article 31
Criteria for Decisions on Personnel Security Clearance

Security clearances shall be issued or renewed only if the individuals concerned pass background checks pursuant to Article 30, see also the criteria set out in this Article, cf. Article 32. When assessing an individual's security competence to handle classified information, the following factors shall be taken into account, as concerns the reliability, integrity and judgement of the individual in question:

a) the fact that he/she has been linked to acts of sabotage, espionage or the organisation thereof, to attempted attacks or other such acts;
b) if he/she has committed a crime or a criminal offence or has abetted others in committing such acts;
c) if certain ties could constitute menace to the individual concerned, or his/her close relatives, that is life threatening, poses a threat to health, inviolability or dignity, and would force him/her to commit acts that could endanger the security of classified information;
d) if he/she has given false or incorrect information or has deliberately suppressed information, which the individual in question should have known that might effect the outcome of an assessment regarding the issue of security clearance;
e) if he/she has a history of alcohol abuse or abuse of other intoxicating agents;
f) if he/she has a disease which, on account of medication, can have effect on reliability, integrity and judgement;
g) if he/she has been involved in compromising classified information, has broken security rules, has refused to furnish personal information about himself/herself, does not authorise the NCIP to conduct checks believed to be important and necessary when background

checks are run, refuses to maintain confidentiality, indicates that he/she does not wish to be subject to confidentiality, or refuses to have an interview with the NCIP;

h) if there a economic factors present that could lead to dishonesty;

i) if he/she has ties with individuals or parties, such as associations, companies, societies or groups, at home or abroad, that have illegal objectives, are capable of threatening democratic societies, or are associated with the organisation, preparation or commission of organised crime, drugs offences, espionage, acts of sabotage or acts of terrorism;

j) there are insufficient opportunities to run a background check;

k) if he/she has ties with foreign countries; and

l) if there are other factors present that might give rise to suspicion that the individual in question might be engaged in activities that could pose a threat to security interests under this Regulation.

A decision to issue or refuse the issue of security clearances, cf. Article 26, shall be based on an informed, clear, objective and individual-based and comprehensive assessment of available information. Political relations, including participation in legitimate political organisations or entities, or in any lawful societies, shall not have effect on the individual's qualification as regards security clearance. Negative information about closely related individuals shall only be taken into account, if their relations are regarded as having effect on the conduct and security competence of the person to be security cleared.

Security clearances shall only be issued after the individuals concerned have received appropriate training from NSA. In specific cases, the NCIP may attach other objective conditions to the issue of security clearances.

Article 32
Assessment of Criminal History

Where background checks pursuant to Articles 30 and 31 reveal that individuals have broken the law, or there is suspicion that they have done so, the NCIP may base its decision to issue security clearance for the individual concerned or not on the criteria set out in this Article.

When decisions are made whether to issue security clearances for particular individuals or not, their criminal records shall be expressly checked. Such decisions shall be based on information collected from judicial records and police case lists, where applicable, and from other police records on the individual concerned, cf. Article 30.

Where an individual has been fined, in Iceland or in other countries, or has been convicted and punished, or where there are pending cases against him/her in the criminal justice system, or where he/she is suspected or accused of committing criminal offences pursuant to Icelandic law, the NCIP shall refuse to issue security clearance for the individual concerned, provided the offences are serious or indicate that the security of the State and/or public interest may be compromised.

Further still, the NCIP shall refuse to issue security clearances if the individuals in question have been convicted of serious offences, e.g. violations of the Penal Code, the use or distribution of narcotic drugs, illegal use of or distribution of weapons, serious violations of the Customs Code, breaches which have endangered the life of a person, acts of violence, blackmail, breaches that endanger the security of the State, sexual offences, and to be or have been members of illegal associations or alleged criminal organisations.

The NCIP may decide to refuse to issue security clearances for individuals on account of other breaches than those listed in this Article and for underlying, objective reasons.

Furthermore, the following circumstances may be taken into account:

a) the individuals concerned have been indicted for a criminal offences assumed to carry imprisonment; or

b) the individuals concerned are wanted by the police, a warrant has been issued for their arrest, or they are subjects of an issue of a foreign travel banning order in accordance with the provisions of the Criminal Judicial Proceedings Act No 88/2008.

The NCIP may decide to refuse to issue security clearances for the individuals concerned, if background checks, cf. Articles 30 and 31, reveal that they have repeatedly been subjects of police intervention on account of their alleged breaches.

Article 33
Repetition of Background Checks

The NCIP is authorised to run repeated background checks on individuals, of its own motion or on application by a competent party and with the individuals' informed consent. In such cases the NCIP may build on available data and information, as far as possible, and may seek further data and information if needed.

Further still, the NCIP may, of its own motion or on application by a competent party, run random checks on those individuals who have passed background checks, as long as their security clearances are valid.

CHAPTER VI
Miscellaneous Provisions

Article 34
Individual's Obligation to provide Information

Individuals, who have received security clearances in accordance with the present Regulation, shall furnish the security officer concerned with information about every aspect that may effect their security competence. The security officer shall inform the NCIP thereof, without delay, who shall decide if there are grounds for withdrawing security clearances of the individuals in question.

Article 35
Further Details on Implementation

When implementing the provisions of this Regulation, the following shall be taken note of, *mutatis mutandis*:

a) The North Atlantic Council's document No C-M(2002)49 of 17 June 2002 on security within NATO;
b) Council Decision (EU) No 2011/292/EU of 31 March 2011 on the Security Rules for Protecting EU Classified Information; and
c) other international agreements and regulations on more detailed elaboration of the above mentioned acts, as the case may be.

Article 36
Confidentiality

Employees of the NCIP shall maintain confidentiality with respect to all information that are revealed in the process of background checking and shall be kept secret.

Access of employees of the NCIP to classified information, cf. paragraph one, is determined by their role within the agency.

Employees, who in the course of their duties gain knowledge of the results of background checks run by the NCIP on individuals, shall maintain strict confidentiality with respect to such knowledge.

Employees, contractors or others, who in the course of their duties gain access to classified information, shall maintain strict confidentiality with respect to such information.

They shall not release to unauthorised parties, and shall be held responsible if they do so, information they receive in the course of their duties, i.e. information that shall be kept secret.

Confidentiality shall be maintained, even if a position is relinquished or after a work contract is completed.

Article 37
Inspections conducted by The NCIP

The NCIP supervises all security factors within organisations and companies with relevance to the implementation of this Regulation, including whether the said organisations and companies discharge their obligations pursuant to laws and regulations; furthermore, the NCIP prescribes improvements.

The NCIP conducts, on a regular basis, inspections of facilities, areas, quarters, installations, tools, information systems or equipment, and other items owned, used or otherwise controlled by an organisation or a company, in order to investigate if unauthorised parties might, with or without the aid of technology, be able to see, hear or read classified information.

In order to be able to conduct inspections successfully, the NCIP shall have free access to any area in which classified information or equipment for handling classified information is stored.

Where inspections, conducted by the NCIP in accordance with the provisions of this Article, reveal that organisations or companies do no longer meet their obligations pursuant to laws or this Regulation, or where remarks need to be made about certain matters, the NCIP shall submit a report on the matter to the party in question, as soon as possible after the inspection has been concluded. The NCIP shall allow for a reasonable amount of time for improvements. If improvements are not brought about within the set time limit, the NCIP may withdraw security clearances and/or security approvals, as laid down in the present Regulation, and shall notify the international organisation concerned thereof, where applicable.

On the average, inspections shall be conducted with 24 months intervals. The NCIP shall issue operational instructions for the conduct of inspections according to this Regulation.

Article 38
Freedom of filing a Complaint

Where the issue of personnel security clearances is refused on the basis of background checks, cf. Article 26, or personnel security clearances withdrawn, cf. Article 28, a complaint may be filed with the Minister for Defence Affairs on the subject of that decision in accordance with the provisions of the Administrative Procedures Act.

Article 39
Sanctions

Breaches of the provisions of this Regulation shall be punishable within the framework of the the following provisions, unless this is subject to more severe penalties pursuant to other laws:

a) the provisions of Chapters XIV and XVII of the Penal Code No 19/1940;
b) the provisions of Article 28 the Defence Act No 34/2008; and/or
c) the provisions of Article 13 of the Act on Control of Services and Items which may have Military Significance No 58/2010.

Article 40
Entry into Force etc.

The present Regulation is adopted in accordance with Articles 24 and 27 of the Defence Act No 34/2008 and with relation to Articles 15 and 18 of the Act on the Rights and Obligations of Government Employees No 70/1996.

The provisions on security clearances of companies with relation to export interests are adopted in accordance with Article 14 of the Act on Control of Services and Items which may have Military Significance No 58/2010.

This Regulation shall enter into force forthwith. Security clearances and/or security approvals in force shall remain in force for the duration of their validity, or until new security clearances and/or security approvals have been issued.

The Ministry for Foreign Affairs, 28 October 2012.

Össur Skarphéðinsson

Einar Gunnarsson

[This translation is published for information only.
The original Icelandic text is published in the Law Gazette.
In case of a possible discrepancy, the original Icelandic text applies.]