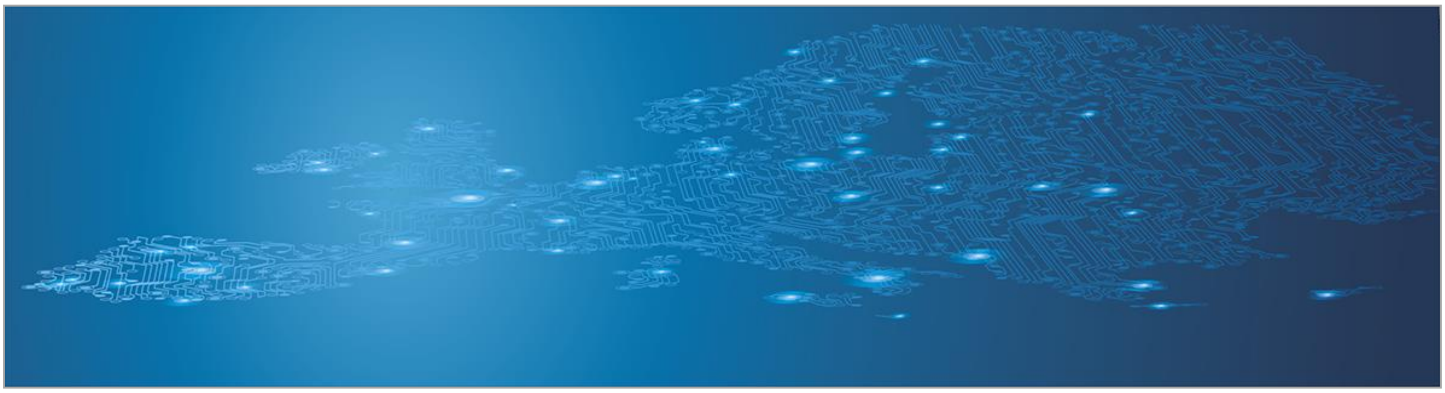

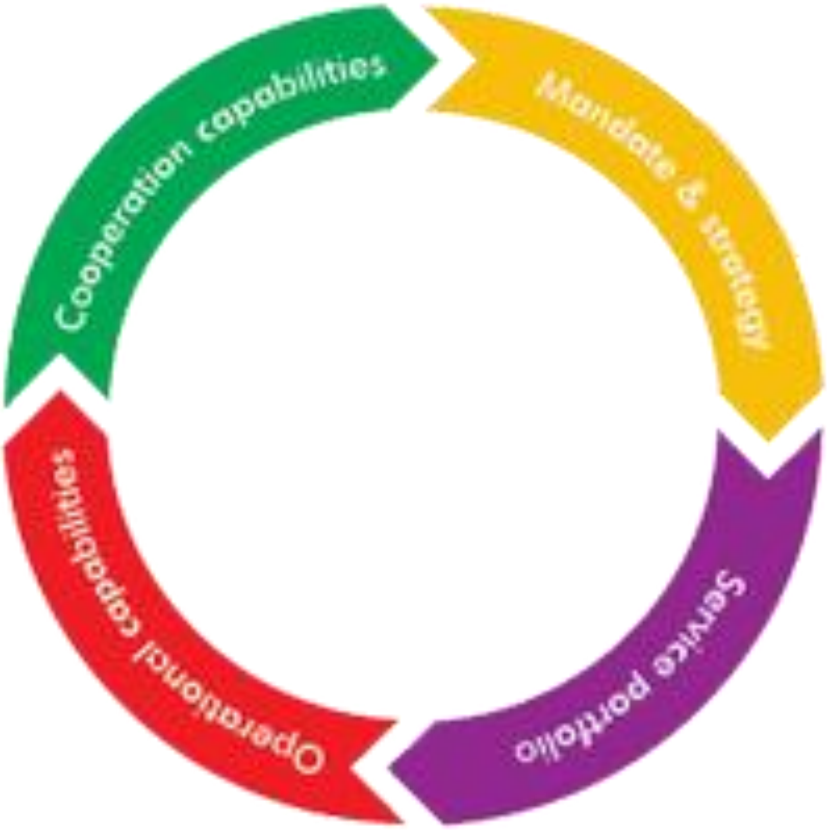

National/governmental CERTs

ENISA's recommendations on baseline capabilities

Update, December 2014

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Andrea Dufkova

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-79-00077-5 doi:10.2788/14231

Executive summary

It is beyond doubt that protection of critical information infrastructure (CIIP), like the internet itself, does not stop at national borders. It is also beyond doubt that in order to effectively and efficientlyrespond to threats and attacks against information infrastructure a coordinated approach at European level is needed. One way to facilitate that goal is to support the Member States in enhancing cooperation among national / governmental CERTs, with regards to information sharing and coordinated incident response.

Due to still existing diversity in capabilities a Europe-wide operational cooperation among national / governmental CERTs, involving stakeholders in all Member States, does not yet exist. However, there are activities and initiatives for information sharing and incident response, which work quite well in practice, and some of them are already active for years.

The experiences gained from these activities provide very valuable insight into cross-border cooperation and the requirements and the obstacles for sustainable information sharing. All future actions at European level to foster cooperation among national / governmental CERTs must take into account experiences made within these successful activities.

Status of this document

The document in its current status is in no way to be considered final, but rather as the record of an ongoing process. This process was started by ENISA in 2009 with a stock-taking survey among all known CERT teams in Europe (in excess of 120 in total) and was, together with the EU Member States and their national / governmental CERTs continued in 2010. This document is therefore to be considered work-in-progress that will undergo necessary changes in the future in accordance with an ongoing dialogue with all relevant stakeholders, which is reflecting the ongoing changes taking place in the European NIS landscape. In some areas of the capabilities of national / governmental CERTs the proposed requirements are quite stable, while in other areas additional research, analysis and comprehensive discussions with the stakeholders involved are necessary. Having a national / governmental CERTs in place that fulfils the requirements for 'baseline capabilities' as defined in this document is essential for CIIP in all Member States. However these teams should not be considered as the one and only necessary measure a Member State must take in order to ensure adequate protection. CIIP at the national level must always be planned as part of a complete cyber-security strategy, in which a national / governmental CERT plays an important role but is not the only component. The planning of a complete national cyber-security strategy in a Member State is outside the scope of this document.

Table of Contents

1 Introduction

Goal

This document covers ENISA's updated considerations for capabilities of so called national / governmental CERTs, thus teams who serve the government of a country to protect critical information infrastructure. National / governmental CERTs play a key role in coordinating incident management with the relevant stakeholders at national level. In addition they bear responsibility for cooperation with the national / governmental teams in other countries.

Target audience

The primary target audience for the updated overview about 'baseline capabilities' in this document are the national/governmental CERTs and those policy-making bodies in the European Union Member States that are responsible for initiating and planning the establishment and operation of a national / governmental CERT and are responsible for creating an adequate national policy framework for these tasks.

2 ENISA's update of national / governmental CERT baseline capabilities

2.1 National / governmental CERTs in Europe

The main goal of a national / governmental CERT, from a cyber-security perspective, is to protect national and economic security, the ongoing operations of a government, and the ability of critical infrastructures to continue to function. Therefore a national / governmental CERT typically handles incidents at a national level, identifies incidents that could affect critical infrastructures, warns critical stakeholders about computer security threats, and helps to build effective incident response across its constituency in both, public and private sectors.

In 2005, ENISA has made its first mapping of existing CERT teams in Europe. In total, there was no more than 100 teams which represented different types of constituencies (e.g. academic, national, private sector). Ten years ago only ten known national/governmental CERTs were established and operational in Europe. Following years the number of teams has grown gradually, but not evenly to a specific region or a country.

Since its establishment in 2005, ENISA has actively supported the process for setting up and developing of new teams in Europe. Strong emphasis has been put on capacity building in the areas of effective collaboration, information sharing and cross-border incident response. It has been identified that effective cross-border incident response and information exchange needs an agreed and common minimum level of capabilities to be accomplished by every participating team.

In 2009, ENISA published a first report on a set of baseline recommendations regarding the minimum capabilities for national / governmental CERT. This document was the foundation for all further activities of ENISA in the area of CERTs like capacity building and trainings, or collaboration between CERTs and law enforcement agencies.

The importance of having a national / governmental CERT in every EU Member State established and operational has been also reflected at the EU policy level recently (e.g. the Digital Agenda, the EU Cyber Security Strategy and in the proposal for a NIS Directive).

The basic service that all CERTs needs to provide is Incident Response, so every team needs to be able to react or respond to security incidents when they happen.

Incident Reporting is a different type of a service that a national/governmental team can offer, which Is of growing importance, as many teams act as national point of contact for incident response coordination (and thus as information hub for teams in other countries, or for stakeholders in its own country). Reporting of incidents also feeds into the various activities for creation of incident statistics, or mandatory reporting according to regulation.

The work of CERTs is delicate and in order to be successful in its daily operations a high level of trust needs to be established with a team's constituents, other teams and non-CERT partners and stakeholders, so it is of utmost importance to have this agreed basic level of functionality and capability.

2.2 Improving national / governmental CERT capabilities – ENISA guidance

The four main categories of capabilities that ENISA defined in 2009 remain unchanged, however, in order to make these categories better understandable also for non-CERT stakeholders like policy makers, we introduce new names in this document.

2.2.1 Formal capability (former 'Mandate and Strategy')

Today policymakers have a better understanding of the importance of and challenges in protecting not only government information but also critical infrastructures that support their economies and the broader public interest within their borders. They are seeking effective and coordinated approaches in their responses to cyber-incidents, threats and attacks that can affect both the public and private sectors. The maturity of national Cybersecurity- and CIIP strategies and the roles of national / governmental CERTs in these strategies are not harmonized between countries and depend strongly on the specific context defined in a country. What is indisputable, however, is that national / governmental CERTs have a key role to play in those strategies from multiple perspectives like information sharing and the coordination of responses to incidents, reporting, etc.

A number of key actions that need to be taken, in order to fulfil this capability:[1]

- An official mandate given by the national government that the team has the capability and the role to officially act and react to cyber security incidents or threats
- A clear definition of roles and responsibilities[2] of the team under the national cyber security policy and legal framework
- Clearly defined relationships with other national stakeholders concerning national cyber security landscape and incident response practice (e.g. LEA, military, ISPs, NSA)
- Stability of the mandate and duration to assure a growing maturity and effectiveness of the team
- Continuity of resources regardless of changes on the national political landscape to assure the continuous incident response capability in the country
- With regard to trust building a clearly defined and broadly communicated role of the team in relation to the host organisation, if any (e.g. Ministry of defence, NSA or top level domain provider) to external parties

Recommended sources for further improvement of the formal capability through EU documentation and ENISA's online good practice library:

- Digital Agenda for Europe (European Commission, "COM(2010)245 at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
- Cyber security strategies in EU MSs – ENISA's overview at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
- Incident reporting and cyber security regulation at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting
- Directive on attacks against information systems – ENISA recommendations for CERTs at http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems
- European CERT community membership at http://www.terena.org/activities/tf-csirt/
- Global CERT community membership at http://www.first.org/members

[1] For more recommendations and details on 'Formal capability' consult http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

[2] See RFC2350 for further details about roles and responsibilities

2.2.2 Operational-technical capability (former 'Service Portfolio')

The service portfolio of any national / governmental CERT will consist of the external services it provides to its constituency and its internal support processes. External CERT services are commonly categorized into three service classes: Proactive, reactive and other security management services.

Reactive services: these services are triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CERT work.

Proactive services: these services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.

The core baseline services for the constituency remain the same as defined in the first report of 2009 3 (incident response, alerts and warnings and announcements). Additional services could be provided to the constituency or to the cooperation partners, like artifact analysis, technology watch or more sophisticated digital forensics analysis for law enforcement agencies in order to support the fight against cyber crime; however, these are optional and do not count to the baseline.

It should be noted that external services still require appropriate internal support processes such as, for example, resource or infrastructure management processes. These supporting processes should also receive adequate consideration as they are the keys to the continuous improvement of the maturity of a national / governmental CERT.

Internal services might be for example a good situational awareness, technical cyber security trainings for staff or participation in various cyber security exercises (e.g. Cyber Europe Exercise).

Emerging new service or customised alerts and warnings?

Cyber threat intelligence is nowadays a popular proactive type of service that a team can offer to its constituency.

The advantage of this service for the team is to be able to issue probability-based warnings of future cyber attacks and tailore alerts and warnings to the specific risks and threats of the constituency.

Cyber Threat Intelligence is an 'evidence-based knowledge including context, mechanisms, indicators, implications and actionable advice about an existing or emerging threat or risk to assets that can be used to inform decisions regarding the subject's response to that threat or risk'4.

Based on the provided definition this service should be considered as a subset of Alerts and Warnings if provided.

Information versus intelligence[5]

Information	Intelligence
Raw, unfiltered feed	Processed, sorted information

[3] http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-for-national-governmental-certs

[4] Description of the term is based on Gartner definition (http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf)

[5] http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf

Unevaluated when delivered	Evaluated and interpreted by trained intelligence Analysts
Aggregated from virtually any source	Aggregated from a reliable source and cross correlated for accuracy
May be true, false, misleading, incomplete, relevant or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy
Not actionable	Actionable

Security quality management services augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organisation such as the IT, audit, or HR departments. If the CERT performs or assists with these services, the CERT's point of view and expertise can provide insight to help improving the overall security of the organisation and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

Recommended sources for further improvement of Operational-technical capability through ENISA's online best practice library:

- CERT tools at https://www.enisa.europa.eu/activities/cert/support/chiht
- Incident management guidance at https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management
- Incident handling automation and data harmonisation at https://www.enisa.europa.eu/activities/cert/support/incident-handling-automation
- Proactive detection of incidents at https://www.enisa.europa.eu/activities/cert/support/proactive-detection
- Alerts, warnings, announcements at https://www.enisa.europa.eu/activities/cert/support/awa
- Actionable Information at https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf

2.2.3 Operational-organisational capability (former 'Operation capability')

In order to operate a national / governmental CERT there is a strong need for appropriate people, technology and processes. Without operational resources such as staff and infrastructure, a national / governmental CERT cannot offer the services discussed in the previous chapter. These requirements has been described in depth in the 2009 report[6]. The essential aspects of operational-orgnaisational capability remain the same: resources, infrastructure, service delivery and business continuity.

Resourcing such as minimum staffing for delivering its services and the budget allocation for the equipment, staff, education also including budget for necessary trust building activities like meetings, workshops and conferences are indispensable elements of well functioning team and trust building for an effective incident response coordination.

[6] http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-for-national-governmental-certs

As a national / governmental CERT is both working for the protection of critical infrastructure of a government and usually acts as a CERT-of-last-resort for all incidents in its constituency, it should be considered mandatory for the CERT to be reachable 24/7/365 by its constituents and its national and international partners.

The requirements concerning confidentiality, integrity and availability of the infrastructure for national / governmental CERTs also remain very stringent because of the role national / governmental CERTs play in crisis situations (eg, large-scale cyber-attacks), the confidentiality of the information processed and stored by a national / governmental CERT (records of incidents, CII vulnerabilities, etc) and because of the criticality of the infrastructure that a national / governmental CERT helps to protect (energy, healthcare, communication networks, etc).

Recommended sources for further improvement of Operational-organisational capability through ENISA's online best practice library and other sources:

- RFC2350 at http://www.faqs.org/rfcs/rfc2350.html
- How to measure cost effectiveness for CERT at http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment
- Overview about the existing EU MS national / governmental CERTs in Annex A
- Recommended check list for publicly available information about the team in Annex B

2.2.4 Co-operational capability (former 'Cooperation')

The security and resilience of national cyber-infrastructure is the joint responsibility of all stakeholders, including operators, service providers, hardware and software providers, end-users, public bodies and national governments. These organisations each have their own roles to play in implementing and operating the national cyber-security, and in order to be effective they must cooperate closely. If national / governmental CERTs are to meet their objectives, sustained and effective cooperation at both the national and international levels is indispensible. Threats, vulnerabilities and subsequent incidents in cyberspace often affect more than one sector or country.

Different situations still require different models of cooperation. A national / governmental CERT can use different procedures to cooperate with a domestic law enforcement organisation or telecom operator than it uses to cooperate with another national / governmental CERT on the other side of the globe. The most important cooperation models remain to be the bi/multi-lateral cooperation and an association or community.

In Europe, a number of national / governmental CERTs have already established relationships with other national / governmental CERTs[7] and with national and international CERT associations[8] and have reached a significant level of maturity, producing high quality responses and information. They have also made bilateral agreements within certain groups on the use of common procedures, terminology, frameworks, standards, etc. Yet a large gap still remains; certain national / governmental CERTs currently lack the maturity or resources to reach these levels of cooperation. In the field, this gap translates into a number of difficulties in incident handling cooperation.

Recommended sources for further improvement of Co-operational capability through ENISA's online best practice library:

[7] http://www.enisa.europa.eu/activities/cert/events/past-events

[8] http://www.terena.org/activities/tf-csirt/ and http://www.first.org/

- Information sharing practice for CERTs at https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing
- Data sharing at http://www.enisa.europa.eu/activities/cert/support/data-sharing
- Secure communication with CERTs and other stakeholders at https://www.enisa.europa.eu/activities/cert/other-work/secure-communication-with-certs-other-stakeholders
- national / governmental CERT annual workshops at http://www.enisa.europa.eu/activities/cert/events/past-events
- European CERT Inventory at https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

2.2.5 Capacity, skills and trust building

As a horizontal task for the overall team's capability the 'Capacity, skills and trust building' capability should be considered by every team.

Expertise skillset of the team members is an important asset for the daily operation of a team especially considering its core services delivery. In order to reach and maintain the expected high level of knowledge and skills in the area of fast evolving cyber security issues a continuous training and education has to be enabled to the team members.

The problem of trust building goes beyond the world of CERTs and can be applied to any community made either of individuals or teams that need to collaborate occasionally. Therefore strong emphasis need to be given to develop this behaviourour type of skills and not only internally within the team, but also with its constituency and the cooperation partners.

Recommended sources for further improvement of capacity, skills and trust building capability.

- CERT training at http://www.enisa.europa.eu/activities/cert/training, cyber exercises at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce and TRANSITS trainings at http://www.terena.org/activities/transits/
- Trust building at http://www.enisa.europa.eu/activities/cert/support/information-sharing/scalable-and-accepted-methods-for-trust-building

3 Future consideration

There is the need to open up national / governmental CERTs to other operational communities[9](e.g. ICS/SCADA[10]) in order to get a better understanding of the work of CERTs on the one hand and the possibilities to cooperate and share information better on the other. The suggested range of stakeholders is as wide as the topics and goal to achieve. This topic will be further elaborated in the upcoming regular update of this document.[11]

[9] http://www.intgovforum.org/cms/170-igf-2014/best-practice-forums-2014/1893-establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security

[10] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc

[11] ENISA WP2015

Annex A

EU MS national / governmental CERTs PoC[12]

EU MS	national/governmental team	PUBLIC WEBSITE
Austria	cert.at/govcert.at	https://www.cert.at/index_en.html ; http://www.govcert.gv.at/
Belgium	cert.be	https://www.cert.be/
Bulgaria	cert.bg	https://govcert.bg/en
Croatia	cert.hr/zsis cert	http://www.cert.hr/ ; https://www.zsis.hr/default.aspx?id=113
Cyprus	Cyprus	http://www.cynet.ac.cy/
Czech Republic	csirt.cz/govcert.cz	http://csirt.cz/ ; https://www.govcert.cz/en/
Denmark	govcert.dk	http://fe-ddis.dk/cfcs/opgaver/govcert/Pages/GovCert.aspx
Estonia	cert.ee	https://www.ria.ee/cert-estonia
Finland	cert.fi	https://www.viestintavirasto.fi/en/informationsecurity.html
France	cert.fr	http://www.cert.ssi.gouv.fr/
Germany	cert-bund	https://www.cert-bund.de/
Greece	ncert.gr	http://www.nis.gr/portal/page/portal/NIS/NCERT
Hungary	govcert.hu	http://www.cert-hungary.hu/en
Ireland	csirt.ie	no public website available
Italy	cert nazionale/cert-pa	no public website available; http://www.cert-pa.it

[12] The list serves only for an overview purposes and cannot be considered fully comprehensive

Latvia	cert.lv	https://www.cert.lv/
Lithuania	cert.lt/svdpt-cert	https://www.cert.lt/en/index.html ; http://www.is.lt/en/svdpt-cert_117.html
Luxembourg	circl.lu/cert.lu	http://www.circl.lu/ ; http://www.cert.lu/
Malta	csirtMalta/govcert.mt	https://opm.gov.mt/en/CSIRT/Pages/CSIRTMalta.aspx ; http://splashpage.gov.mt/
The Netherlands	ncsc.nl	https://www.ncsc.nl/english/organisation
Poland	cert.pl/cert.gov.pl	http://www.cert.pl/ ; http://www.cert.gov.pl/
Portugal	cert.pt	http://cert.pt/en/
Rumania	cert-ro	http://www.cert-ro.eu/index.php?lang=en
Sweden	cert.se	https://www.cert.se/
Slovakia	csirt.sk	https://www.csirt.gov.sk/
Slovenia	si-cert	https://www.cert.si/en/
Spain	ccn-cert/certsi	https://www.ccn-cert.cni.es/ ; https://www.incibe.es/CERT_en/Critical_Infrastructures/
United Kingdom	cert-uk	https://www.cert.gov.uk/

Annex B[13]

Basic set of information that should be publicly available about every EU MS national / governmental CERT team and in English language:

- Contact address
- Time zone
- Telephone number
- Abuse/notification mail address
- Encryption information/public key
- Response time
- Office hours
- 24/7 reachability status
- Public website
- Definition of the constituency
- Reporting authority
- TI accreditation/certification
- FIRST membership
- Official mandate
- Services provided
- Incident reporting forms

[13] According to RFC2350 documentation

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu