# GFCE Global Good Practices

## National Computer Security Incident Response Teams (CSIRTs)

GFCE
Global Forum on Cyber Expertise

# Preface

The unprecedented uptake of information and industrial control system/operational technologies (IT and ICS/OT) worldwide leads to a growing dependency of economic sectors, public institutions and societies. Nowadays, threat actors target specific individuals, organisations, industries, and nations, or may indiscriminately target any system. Therefore, it is crucial for nations to take their responsibility and build an effective capacity to prevent, react promptly, and recover quickly from cyber incidents at the national level. Such a capacity which - collaborates and coordinates with national and international communities and organisations - is often referred to as 'national Computer Security Incident Response Team' or national CSIRT.

The UN Group of Governmental Experts on Developments in the field of Information and Telecommunications in the context of international security referred to national CSIRTs in its (UN GGE, 2015) report and encourages all nations to establish a national CSIRT.[1] In addition, various regional cyber capacity building initiatives (e.g., OAS, EU) acknowledge the importance of having a national CSIRT.

The concept of CSIRTs grew out of the collaborative experiences gained by organisations during the response to the Morris Worm which brought down the Internet on November 2, 1988. The first computer incident response teams were established by academic communities; over time the need and value of CSIRTs has become clear. Currently, CSIRTs exist at the level of individual organisations, IT- and ICS-manufacturers[2], sectors, nations and international organisations.[3]

National CSIRTs provide the capability of fast, integrated and coordinated cyber incident response for your national sectors and cyber dependent communities, the nation at large, and in support of the international community. The latter works reciprocal in case your nation needs support.

Therefore, political leadership and government policy-makers in nations are encouraged to establish a well-embedded, connected and matured national CSIRT capacity by adopting the steps and good practices outlined in this document. Doing so is one of the essential boundary conditions in building a secure and resilient cyberspace that serves its citizens.[4]

The good practices and list of references in this document stem from earlier studies and literature; evidence-based experiences provided by international organisations (e.g. ENISA, ITU, OAS), mature national CSIRTs, and CSIRT communities (e.g. FIRST, APCERT, LACNIC AMPARO, OIC-CERT, TF-CSIRT), as well as the outcomes of GFCE expert meetings on CSIRT Maturity held in Prague (January 2016), Seoul (June 2016), and Geneva (October 2016).

1 The UN GGE is the leading international community's efforts in negotiating global cybersecurity norms under UN's auspices.

2 For example, Product Security Incident Response Teams (PSIRT).

3 For more for background on history, types and culture of CSIRTs in general, see (Morgus et al., 2015a).

4 Cyberspace is the conglomerate of IT tools and services and comprises all entities that can be or are digitally linked.

# 1. Introduction

## Why does every nation need a national CSIRT capacity?

Even the best cyber security posture and practices cannot guarantee that key organisations and information infrastructures within a nation will not be vulnerable to malware, software failures, human errors, and other mishaps. The cyber threat landscape changes rapidly. Cyber incidents occur on a daily basis and may be of cross-border, multinational and often even global nature. Nowadays, threat actors target specific individuals, organisations, industries, and nations, or may indiscriminately target any system. Therefore, it is crucial for nations to take their responsibility and build an effective national CSIRT capacity. We will regularly refer to this capacity as "national CSIRT" in this document for the sake of simplicity, but remember that this national CSIRT may be one team, or consist of multiple teams with national responsibility: one approach is not necessarily better than the other.

The preparedness and readiness as well as the speed at which a nation can address and react to cyber threats and incidents, limit the damage, lower the cost of recovery, and keep the societal trust in cyberspace high. An organisationally, legally and internationally well-embedded, well-trained, and otherwise mature national CSIRT provides such a key societal role both nationally and as part of wider national and global communities. In the case of smaller countries, where the funding of an effective separate national CSIRT capacity may be an issue, it should be considered if there is a suitable party to subcontract this function to.[5]

## What is a national Computer Security Incident Response Team?

A national Computer Security Incident Response Team (CSIRT)[6] is an operational entity that:

- has a national scope,
- is recognised by the national government,
- is tied into the national crisis management structure,
- operationally cooperates with multi-stakeholders on countering cyber threats and incidents, nationally, bilaterally and internationally,
- collaborates with other national and or regional CSIRTs, governmental CSIRT(s), product security teams of manufacturers/vendors (known as PSIRTs), and leading international communities to advance CSIRT governance, legal frameworks and capacities,

[5] Examples are Slovenia, the Czech Republic and Austria. In Slovenia, the national research network has this role. In the other two examples, it is the top-level domain (.cz and .at) provider.

[6] Some other notions equivalent to CSIRT are: Computer Emergency Response Team (CERT), Computer Incident Response Capability (CIRC), Cyber Incident Response Team (CIRT), Computer Security Incident Response Capability or Centre (CSIRC), Computer and Network Security Incident Response Team.

- usually is the national point of contact for CSIRTs from other nations and supranational bodies,

and provides *as minimum* the following core elements of operations/services:

- cyber-related incident management (activities aimed at preventing and resolving cyber security incidents, and presenting lessons learnt in the process),
- outreach to and communication with its constituency [7],
- situational awareness about cyber security risk.

In addition to national CSIRTs, there could be other types of CSIRTs whose serve constituencies in critical infrastructure sectors, universities, financial institutions, the government and its agencies, municipalities, product manufacturers, cyber industry, and other types of organisations. The national CSIRT will closely collaborate with many of those organisations and communities, see *Good practice 6: Link up with other CSIRTs*.

## Why is a sufficient maturity level of the national CSIRT important?

Cyber security is not just a national, but indeed a regional and global effort. Incidents usually cross many borders, both of organisations and of nations. Therefore, the only way that national CSIRTs can be effective in preventing and resolving the cyber security incidents is to collaborate locally, nationally and globally. National CSIRTs need to achieve a level of maturity that is *sufficient* to allow them to share and contribute in a meaningful way to be truly effective. Such a *sufficient* level of maturity is also a requirement to gain trust from fellow national CSIRTs. Therefore, it is necessary to define how the maturity of a national CSIRT can be assessed and increased (see Good practice 1: Measuring maturity).

[7] Constituency refers to the set of organisations or entities being supported and serviced by the national CSIRT capacity.

# 2. Good Practices

## Step-by-step approach for creating the national CSIRT capacity

The need for a national cyber incident response function expressed in chapter 1 would preferably be underpinned by a national risk assessment. Having its functions clear, the need and embedding of a national CSIRT capacity in the national organisational structure preferably should be part of the National Cyber Security Strategy, national IT strategy, and or cyber-related law and regulation.

A step-wise approach can be used to create the national CSIRT capacity. In summary, the following steps and activities can be recognised in the set of older and recent good practice documents such as (ENISA 2006-2011), (Killcrece, 2004), (West-Brown, 2003), (Organization of American States, 2016), and (CERT/CC, n.d.):

1. Develop a strategy and cover the following strategic matters:
   - Is there a national cyber security strategy? The national CSIRT should be part of that.
   - What is the mission of the national CSIRT? What particularly is its role in the national strategy?
   - What is the constituency, and who are the stakeholders? Educate stakeholders if needed.
   - What kind of authority and responsibilities does the CSIRT have towards their constituency?
   - What should the governance model be? (including high-level support, sponsorships, financial embedding/funding, auditing).

2. Create a charter or "business plan" of the national CSIRT capacity to get approval from the highest governance and political levels, paying attention to:
   - Mandate, mission, constituency, authority, responsibility as defined under strategy.
   - Maturity framework to measure and improve maturity.
   - Organisational, management and financial structure.
   - The range and (quality) level of services the national CSIRT will offer.
   - Staffing model, education & training.
   - National and international co-operations and memberships.
   - The CSIRT's communication matrix and information flows.
   - Fundamental policies (confidentiality, ethics, dealing with the press, etc.).
   - Distilling lessons learnt, reporting and auditing.
   - Accountability and supervision.

3. The implementation & Operation model should pay attention to the following issues:
    - Gaining & training staff, defining roles and responsibilities.
    - The resources needed such as equipment, tools, and infrastructure.
    - The context of laws and regulations for the CSIRT (e.g. data / privacy protection, monitoring, reporting, data sharing).
    - Processes, and especially the incident management process(es).
    - Getting to know and working together with the constituency and other stakeholders.
    - Gain visibility nationally and internationally. Participate in relevant CSIRT forums.
    - Contingency planning for the national CSIRT.

4. Build up a trust relationship to your constituency and important stakeholders:
    - Seek contact to your constituency and build up a trust relationship. This is challenging if the CSIRT in fact is a government entity.
    - Identify important stakeholders in your region of activity, such as other CSIRTs or PSIRTs.
    - Define how to collaborate and share the burden of the information handling among the players. Much is gained by using synergies.
    - Ensure that no competition to private sector initiatives is created, as this is unconstitutional in many jurisdictions.

5. Continuous improvement: the national CSIRT must continuously improve and re-invent itself to be flexible enough to deal with the ever-changing threat landscape worldwide. To do so, pay attention to at least the following:
    - Participate and invest in exercises and “fire drills” on the level of the national CSIRT itself, on the broader level of constituency and nation, and even internationally.
    - Keep measuring the national CSIRT’s maturity level, and the quality levels of the services it has chosen to provide. External assessments can help gauge quality.
    - Make sure that the national CSIRT staff members regularly discuss the latest threats, incidents and trends – to derive lessons learnt. Make sure there are multiple channels for sharing those.
    - Cooperate nationally with constituency and stakeholders, and learn from each other.
    - Contribute to the regional, sectoral and global co-operations of CSIRTs and send people there. This investment pays itself back over time, as it brings in valuable knowledge, expertise and “networking”.
    - Institutionalise knowledge, experiences and relationships through documented policies, procedures, guidance, workflows, and interfaces.

Various steps in the above lists are singled out in more detail as good practices below.

## Foundation of the national CSIRT capacity

Before establishing the national CSIRT, it is important to have a firm foundation. Good building blocks upon which the national CSIRT capacity can be founded are a clear mandate, solid embedding at the political and governmental strategic level, long-term funding, understanding the constituency, the authority and responsibility towards that constituency, and capacity building with international support. Following these good practices, the national CSIRT will have a solid basis to build on.

***Good practice 1: Establish the right mandate***

The national CSIRT can only be effective if there is a clear and official right to operate. The mandate of a national CSIRT ideally emerges from the national cyber security strategy or NCSS (ENISA, 2016) and could be laid down in law or regulation. The NCSS describes the national high-level approach to cyber security establishing a range of objectives and priorities to be achieved in a specific timeframe. The mandate defines the assignment of the CSIRT. Ideally, the mandate is set at the highest management or political level, and may be anchored in legislation (ENISA, 2017).

***Good practice 2: Ensure top-down embedding***

A national CSIRT capacity is an operational entity delivering services to its constituency. The national CSIRT capacity interacts with other CSIRTs, nationally and internationally, and has direct links to national emergency management at the strategical and tactical levels. The national CSIRT capacity should be politically and governmentally endorsed and have -if necessary- a legal underpinning. Moreover, a well-established connection with the national crisis management structure is necessary to be able to upscale the national CSIRT's operations in times of crises. In other words: the set-up of the governance and accountability for the national CSIRT is very important.

***Good practice 3: Establish the national CSIRT's constituency, authority and responsibility***

*Constituency* comprises the group(s) that the national CSIRT capacity aims its service and support at, in other words "its clients" (e.g., governmental organisations, critical infrastructures, municipalities, citizens). The national CSIRT interacts with a wide range of entities and communities of which its constituency and other CSIRTs in the nation are the most important. Closely related to the constituency are the authority and responsibility of the national CSIRT capacity taking into account existing CSIRTs.

*Authority* is the extent to which the national CSIRT can act toward and for its constituency given its role and mandate (Stikvoort, 2008). This authority could vary from advisory, toward enforcement or escalation options. For example, a national CSIRT may work with an internet service provider to prevent further damage – or instead it may only have an escalation or alarming possibility. It is a good practice to define the authorised abilities upfront rather than debate them during an emergency.

The national CSIRT's *responsibility* describes the role(s) and expected actions in preventing, mitigating, investigating and responding to cyber incidents given its mandate. For example, a national CSIRT may be expected to provide cyber incident management at the national level, broadening incident response in private sectors, and training.

It needs to be stressed here that two of the most important values for any national CSIRT should be cooperation and transparency. To be successful in the complex matrix that exists in any given country, the national CSIRT capacity needs to "work together" and facilitate rather than take a top-down approach. Transparency means that the national CSIRT capacity, as any CSIRT, needs to "give and take". Only by the willful sharing of information, can the CSIRT cooperation reach its highest degree of success – secretive approaches have proven time and again to fail in the national and global CSIRT cooperations.

***Good practice 4: Seek support from others for national CSIRT capacity building***

The national CSIRT is encouraged to use the knowledge and expertise readily available in international communities for its foundation. Global and regional communities exist that share practical and applicable solutions to incident prevention and resolution. The most important global community is the Forum of Incident Response and Security Teams (FIRST). However, in every region there exist one or more regional communities that could be very valuable to join.[8] Additionally, *sectoral* cyber incident information sharing communities also exist internationally.

Moreover, bilateral or multi-lateral coaching relationships may be beneficial to consider when building the national CSIRT capacity. Nations with less developed cyber security incident prevention and response capacities can learn from a buddy nation about valuable organisational or process-wise approaches and about pitfalls to avoid. The Meridian process buddying initiative follows a capacity building approach whereby a nation may consider engaging as a buddy nation (or a guide nation). This initiative may be linked to other national CSIRT capacity building arrangements, see the Annex.

Beyond coaching, many CSIRTs work together on various projects, thus pooling expertise which is often rare. It can be highly beneficial to seek such pooling arrangements with other CSIRTs.

[8] For an extensive list, see section 2.4 *National and international co-operation* in "CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity" (NCSC-NL).

## Establishing the national CSIRT capacity

To establish a national CSIRT and making it operational in an effective way in the national context, a set of pre-conditions needs to be well-understood and satisfied. These aspects are outlined below.

***Good practice 1: Well-thought organisational positioning***

A national CSIRT capacity needs operational communications with all relevant governmental stakeholders, from law enforcement, national crisis management to cyber policy-makers, and national intelligence/security services. A national CSIRT should be organisationally positioned in such a way that its operations can take full advantage of the nation's organisational structure. Consider the challenges listed in Chapter 3 below when establishing a national CSIRT and ensure that the national CSIRT is:

- strategically and tactically endorsed by the government, e.g. being established by law or presidential decree,
- well-connected with the national crisis management structure,
- available as an international point of contact for cyber security incidents,
- well-linked or liaised with all the national stakeholders, and
- established in a way that it can operate effectively.

National CSIRTs can be found in organisations such as the national crisis/emergency response agency, ministry of Interior, national intelligence/security agency, defence organisation, governmental IT services agency, and national telecom regulator. National CSIRTs are sometimes established as private organisations, e.g. within domain registrars.

***Good practice 2: Decide on the set and scope of national CSIRT services***

Right from the start it should be clear which services the national CSIRT intends to deliver. The CSIRT Services Framework (FIRST, 2017) is a good practice to design and develop CSIRT services and functions. This framework uses community-accepted terminology and facilitates the establishment of CSIRT operations, capability development, and education and training. The framework recognises the following service areas and services:

1. **Incident management** (incident handling, incident analysis, mitigation and recovery) which comprises activities aimed at preventing, mitigating against, preparing for, coordinating response / responding to, investigating, and recovering from an incident (CIPEdia),
2. Analysis (artefact analysis, media analysis, vulnerability / exploitation analysis),
3. Information Assurance (risk assessment, operating policies support, business continuity and disaster recovery planning support, technical security support, patch management),
4. **Situational Awareness** (metric operations, fusion and correlation, development and curation of security intelligence),
5. **Outreach/Communications** (security awareness raising, cybersecurity policy advisement, Information sharing and publications),

6. Capability Development (organisational metrics, training and education, conducting exercises, technical advice, lesson learned),
7. Research and Development (development of vulnerability discovery / analysis / remediation / root cause analysis methodologies, development of technologies and processes for gathering / fusing / correlating security intelligence, development of tools).

At a minimum, the national CSIRT shall start with the provision of the three services printed in **bold**. It is recommended to start with a small operation delivering the minimum set of services well to build trust and confidence amongst the sets of stakeholders. Additional national CSIRT services can be added when the organisation is prepared for and able to step up to the next level. The requirements and needs of the constituency shall be considered, as well as the services provided by other CSIRTs.

***Good practice 3: Explore the operational legal boundaries of the national CSIRT***

National CSIRTs operate in an environment bound by legal constraints such as data protection, personal data/privacy protection, civil liberties, powers of investigation, and national security (see Chapter 3 – Key challenges). In the start-up phase national CSIRTs should walk through characteristic threats and incident scenarios to explore the (legal) boundaries of their operational space together with their legal advisors, law enforcement agencies, and intelligence/security services. Knowing these boundaries eases operations and operational speed as lengthy discussions with legal advisors and operational people can that way be avoided in times of crisis. Moreover, identified barriers for effective operations may be removed or partially relieved by special national CSIRT related regulations and agreements.

***Good practice 4: Consider the constraints of freedom of information acts, privacy, liability and the concerns of information sharing entities***

As part of their mandates, a national CSIRT may acquire, receive, process and possess (inter)nationally classified information, commercially sensitive and privacy sensitive data from public and private parties. The possible leakage of sensitive information via a Freedom of Information Act (FoIA) may cause the constituency and other collaborating parties to be concerned and reluctant to share cyber security-related incident information. Leakage may damage (national) reputation, disadvantage market positions, intellectual property rights (IPR), and reduce the stock value. Therefore, the physical, cyber and personnel security of the national CSIRT must be able to deal with the highest level of confidentiality of information expected to be handled and processed. A practice is that nations make an exemption in the FoIA for sharing with the public all voluntary shared cyber threat and incident information in possession of the national CSIRT. For the constituency, collaborating organisations of a national CSIRT and parties involved in for instance *Coordinated*

*Vulnerability Disclosure* (GFCE, 2017), it should be crystal clear how sensitive cyber threat and incident-related information is processed, stored and shared.[9]

When dealing with the resolution of cyber security incidents, the national CSIRT may collect and process personal identifiable information. Practically, it is impossible for the national CSIRT to know beforehand the detailed kind of information that will be collected and processed during crises or incidents, although one can be prepared for generic types of identifiable information. Therefore, the national CSIRT may not be able to satisfy all legal requirements of national and international data protection (privacy) laws and standards. Proper security measures and specific arrangements with the data protection entity or regulator should be made ensuring the ability to perform the national CSIRT's tasks.

Liability becomes relevant whenever an action – or lack thereof – can cause harm. Part of the business of any national CSIRT may be to advise its constituency to take (or not take) specific actions. Most often, the national CSIRT cannot wait for full legal clearance until they issue advice, as that would simply take too long. However, there is always a risk that such actions backfire and cause some form of harm, usually in terms of cost and reputation. Thus, liability is always a potential risk – and especially for national CSIRTs it is recommendable to come to some kind of special stature on the longer run.

Last but by no means least, the concerns of information sharing entities need to be taken into account. Some organisations, private or otherwise, may not wish to share if they do not understand how the information will be used. For instance, when a software vendor passes along information to a national CSIRT, it should be clear that this information is provided for remediation purposes. In some cases, this information may be useful for prosecution, or even for offensive purposes. Vendors will be more incentivised to share when they have a good understanding of how the information they may provide will be processed and used.

***Good practice 5: Build communities***

A national CSIRT capacity benefits from building and maintaining trust (see chapter 2) with its constituency and its other stakeholders, which takes time and is a continuous effort. Constituency relationship management, targeted workshops and joint exercises will help to build and mature the community. A national CSIRT capacity can only really thrive in a spirit of co-operation and (relative) transparency, as it should work with a multitude of constituents, stakeholders, other CSIRTs, agencies etcetera. In many cases, the collaboration will be on a voluntary basis. It has been proven over the past decades that such collaborations are only successful when all sides willingly share information (threats, incidents, methodologies), see (Luiijf and Kernkamp, 2015). This give-and-take approach is essential to the way that the global CSIRT community functions, it is like a life-breath.

[9] See "Freedom of Information Act (FoIA)" in (Luiijf and Kernkamp, 2015).

This also means that the importance of community building extends to the supranational level. To invest in this community building is of vital importance to the success of any national CSIRT.
Moreover, the national CSIRT's (professional) operational decisions should be separated as much as possible from possible (non-technical) political effects and influences. The national CSIRT needs to be seen - both nationally and internationally - as a trustworthy partner which is politically neutral, unbiased, and professionally/technically driven, as much as possible.

***Good practice 6: Link up with other CSIRTs***

Apart from its primary constituency, a national CSIRT capacity may become, in close collaboration with the other national stakeholders, the national focal point for the cooperation of CSIRTs and Information Sharing and Analysis Centres (ISACs) of large organisations, critical infrastructure operators, economic sectors and branches, municipalities, and so on. A good practice is that a national CSIRT capacity stimulates the establishment of such CSIRTs and ISACs by providing tools, guidance and good practices, expertise, and organising joint exercises. Already existing CSIRTs could be connected by building trust and providing reliable arrangements for optimal information exchange. In that way, the national CSIRT capacity can in fact be extended by sharing the capacities of other CSIRTs.

## Co-operation & building and maintaining trust

Cooperating nationally as well as internationally is not only a means to gain experience and knowledge; it is also an essential component of trust building. The importance of this cannot be overestimated: it is crucial for the mid- and long-term effectiveness of any national CSIRT capacity. Trust building is a continuous effort, and should therefore be self-maintaining. Do bear in mind however that trust is gained slowly, but can be lost overnight. It is also important to understand that “trust” between CSIRTs in this community is based on the sum of the trust relationships between individuals working for these CSIRTs – and therefore the establishment and maintenance of trust relationships with members of other (national) CSIRTs is not just a nice-to-have: it is a priority. Note that legal agreements are necessities in certain situations, but by themselves they do not create trust.

***Good practice 1: National co-operation & trust building***

The national CSIRT capacity collaborates with constituents, other CSIRTs and stakeholders in their own nation. To work together and build trust, consider taking the following approaches:

- Organise and facilitate a national co-operation and meeting of CSIRTs from all sectors.
- Organise and facilitate an operational co-operation between the CSIRTs that serve the nation's critical infrastructures.
- Organise annual workshops or conferences for constituency and stakeholders. It is advisable to also invite national and international partners, as this will improve the quality of the event, plus make clear to all that cybercrime fighting is not a national, but a global effort.
- Organise and/or participate in national scale exercises and fire drills. Facilitate the participation of other CSIRTs in international exercises.
- Participate in existing meetings and forums of CSIRTs to build trust and strong relationships.
- Having co-operation and meetings with the national crisis management structure.

***Good practice 2: International co-operation & trust building***

As argued before, it is essential for any national CSIRT to position themselves as active members in relevant supranational CSIRT co-operations. The following is a recommended practice:

- Become a member of FIRST, the worldwide forum for CSIRTs, and contribute actively there. FIRST organises an annual conference, and many regional meetings and trainings. FIRST also features working groups that deal with various aspects and standards that matter to all CSIRTs (FIRST).
- Join the CSIRT co-operation in your geographical region, e.g. GEANT TF-CSIRT in Europe and APCERT in the Asia-Pacific area. As a rule of thumb, national CSIRTs will join both FIRST and regional co-operations. [10]
- Join any sectorial co-operations that may be relevant to your national CSIRT, like in the energy or financial sectors including but not limited to ISACs.
- Participate in joint exercises organised by the various co-operations.

## Maturing the national CSIRT capacity

CSIRT maturity is an indication of how well a team governs, documents, performs and measures its own operation. Any national CSIRT needs to apply a maturity framework to be able to assess their maturity level and compare it with other national CSIRTs.

[10] For an extensive list, see section 2.4 *National and international co-operation* in (NCSC-NL, 2015).

***Good practice 1: Measuring maturity***

The most popular maturity model for CSIRTs is SIM3: Security Incident Management Maturity Model (Stikvoort, 2008). SIM3 is freely available from the not-for-profit Open CSIRT Foundation (OCF), which is responsible for maintaining and improving the model and organising trainings for SIM3 assessors.

SIM3 exists of 44 maturity parameters in the fields of organisation, human aspects, tools and processes – each of which can be measured on a maturity scale that ranges from zero to four; four being most mature. ENISA, with help of the OCF, have developed a questionnaire that national CSIRTs can use to do a self-assessment of all these parameters (ENISA, 2017).

SIM3 is the basis for the existing Certification process for European CSIRTs. Other national CSIRTs started to adopt SIM3. An example is the Japanese CSIRT co-operation NCA which has adopted SIM3 for measuring and improving maturity; other major players like FIRST are incorporating SIM3 in their maturity strategy.

Based on the SIM3 framework, the *CSIRT Maturity Kit* has been developed to assist emerging and existing CSIRTs to increase their maturity level. This is achieved by offering a set of good practices that cover CSIRT governance, organisation and operations. These good practices cover the areas described in this Global Good Practice – and more. The CSIRT Maturity Kit is subject to regular updates (NCSC-NL, 2015).

***Good practice 2: Improving maturity***

The CSIRT Maturity Kit gives general pointers that will help improve maturity. A more structured approach is to use SIM3 directly for assessments and then comparing the results with a minimum set of requirements as is the case for the European Certification, which is performed by an independent entity (Trusted Introducer, 2009-today).

Another option is to define a maturity growth path. The latter approach has been adopted by the CSIRT's network, the co-operation of the national CSIRTs of the EU member states, who have defined a growth path based on SIM3 that goes from "basic" maturity level, via "intermediate" to "certifiable" (ENISA, 2017). Measurements here are planned to be based on a combination of self-assessments and peer reviews. Different communities of CSIRTs can of course make their own choices in regard the SIM3 levels that they want to achieve – although some level of commonality in regard maturity at least between national CSIRTs worldwide would be helpful.

The use of the SIM3 is a good example – key is to establish a repeatable methodology and set of criteria for evaluating your CSIRT, incorporating lessons learnt and addressing gaps that are identified. Other evaluation instruments can be used.[11]

[11] See e.g. references in the CSIRT Maturity Kit.

# 3. Key challenges

***Key challenge 1: Unclear mandate, authority and responsibility***

Lack of clarity about the mandate and role of the national CSIRT capacity will inevitably turn into confusion during and outside crisis situations. The national CSIRT should formally announce its mandate, authority, responsibility, and CSIRT cooperations to its constituency and other CSIRTs. A national CSIRT should assure that these are well understood. Especially during start-up, it is essential to narrow the scope and support only a necessary minimum constituency with a set of services such as national CSIRTs at least provide.

***Key challenge 2: Organisational positioning***

The organisational positioning of a national CSIRT is a challenge for each nation. For example, if the national CSIRT is a private entity, the national CSIRT may be hampered in its information flows from national government agencies and foreign national CSIRTs being considered less trustworthy. If a national CSIRT is positioned with or close to national intelligence/security services, the nature of such an agency may be restrictive to the necessary sharing of cyber-security related information with non-intelligence/security service communities such as foreign national CSIRTs.

Although a national CSIRT is an *operational* level entity, it needs strong links with strategic/tactical elements of the government. Unwise positioning, lack of governance, or not recognising its special tasks by submerging the national CSIRT in an existing governmental entity may cause malfunctioning (Luiijf and Healey, 2012). Therefore, when organisationally positioning the national CSIRT, it is essential to meet the challenges of balancing the long-term pros and cons with current organisational structures and mandates.

***Key challenge 3: Constituency building***

In the drive to create a constituency, public authorities may make the mistake to think that organisations such as critical infrastructure operators are automatically prepared to start cooperation with them. It takes time to find the right point of contacts within specific organisations and build trust before a fruitful cooperation can be established. Sufficient time and capacity must be available to do this stakeholder management right. This process always takes more time than estimated beforehand.[12]

***Key challenge 4: Liaisons and stakeholders may face conflicts of interests***

Law enforcement, national intelligence/security services, and alike liaisons to the national CSIRT may have multiple conflicting tasks and role ambiguity. When sensitive threat and incident information is shared by the constituency or international partners, such liaisons may be obliged by the national legal framework to switch roles and act accordingly, by that ignoring, circumventing or even "abusing" the national CSIRT and its trust building processes due to other operational policies and

[12] Based on "Embed at the top", Sharing Cyber Security Information (Luiijf and Kernkamp, 2015).

priorities.

At one end of the spectrum sensitive information may become national classified information, e.g. as information within an investigation or as part of national security. It will become hard to use and share such information. Moreover, such agencies may 'lock up' and end sharing valuable information available at their side (Luiijf and Kernkamp, 2015). The solution here is not "more rules" but instead build close trust relationships and make clear what information will be used for what purposes.

***Key challenge 5: Legal interference***

The national CSIRT may be hindered in performing its tasks when legal issues take prominence. For instance, disagreements over who owns the data and intellectual property. And, as intrusion detection information may reveal privacy sensitive information of a cyber attacker, in some nations a national CSIRT may not be allowed to merge cyber-attack data collected by different governmental agencies. Such frictions may cause crucial delays in providing information to the constituency and reduce the national CSIRT's effectiveness.

***Key challenge 6: Lack of resources***

Funding of a national CSIRT capability is considered a key challenge in many nations. It is still hard to justify the costs with the benefits of preventing and mitigating incidents which may have a large effect upon the national critical infrastructure, its economy, and its organisations and citizens.

***Key challenge 7: Finding and retaining qualified staff***

With the deficiency of well-trained professionals, it can be difficult to find and keep qualified staff in the field of cyber security, given the scarcity of available qualified professionals on the very competitive cyber security labour market in most nations. Staff should be cross-trained, preventing 'single points of failure' should someone performing a function requiring a unique skill set leaves the national CSIRT. Also, salaries should be competitive enough to support keeping the staff. On the other hand, recruitment by the national CSIRT should pay attention to not drain too many human resources jeopardising the cyber security posture of organisations that are vital to the nation.

***Key challenge 8: Scalability during crisis***

The development of crisis cannot be foreseen. When 'all hands on deck' are required around the clock, resources of the national CSIRT capacity may run short unless additional staff or capacity can be mobilised, e.g. from other CSIRTs. As all communication of a national CSIRT with other stakeholders require IT-based resources, ongoing attacks involving public operators (and probably the national CSIRT itself too) will create a challenge to always have means of communication available in times of crisis. It is recommendable to investigate and invest in redundant ways of communication, and not to wholly rely on IT alone.

# Annex: sources on (national) CSIRTs and related good practices

The following sources were used to develop this Global Good Practice and may be of use for policy development and implementation by individual governments and or critical (information) infrastructure operators and other stakeholders.


CERT/CC Action List for Developing a CSIRT and Create a CSIRT. Retrieved from: http://www.cert.org/incident-management/csirt-development/action-list.cfm and http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

CIPedia© (2017). CIPedia is a web resource on international CIP and CIIP related definitions and abbreviations by the EU CIPRNet project. Retrieved from: http://cipedia.eu

European Union Agency for Network and Information Security (ENISA), (2006-2011). CSIRT Setting up Guide – available in all EU member state languages (including French, English, German, Italian and Spanish), plus Chinese, Hindi and Russian). Retrieved from: https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building?tab=publications

European Union Agency for Network and Information Security (ENISA), (2015). Leading the way: ENISA's CSIRT-related capacity building activities, ENISA, Heraklion, Greece. Retrieved from: https://www.enisa.europa.eu/publications/leading-the-way-enisa-s-impact-in-operational-security/at_download/fullReport

European Union Agency for Network and Information Security (ENISA), (2016). NCSS Good Practice Guide. Retrieved from: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

European Union Agency for Network and Information Security (ENISA), (2017). Study on CSIRT Maturity – Evaluation Process. Retrieved from: https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process/at_download/fullReport

FIRST (global Forum of Incident Response and Security Teams) repository of CSIRT-related documents. Retrieved from: https://www.first.org

FIRST CSIRT Framework, v1.1 (2017). Retrieved from: https://www.first.org/education/csirt_service-framework_v1.1

GFCE (2017). Memorandum on Good Practices for Coordinated Vulnerability Disclosure (CVD).

Killcrece, G. (2004), Steps for Creating National CSIRTs, CERT CSIRT Development Team, Carnegie Mellon University, Pittsburgh, USA. Retrieved from: https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

Luiijf, E. and Healey, J. (2012). Organisational Structures & Considerations, in: Klimburg, A., National Cyber Security Framework Manual, NATO CCD-COE Publications, Tallinn, Estonia. Retrieved from: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Luiijf, E. and Kernkamp, A. (2015). GCCS2015 Good Practice: Sharing Cyber Security Information, TNO. Retrieved from: DOI: 10.13140/RG.2.1.4321.7442 https://repository.tudelft.nl/view/tno/uuid:1eeb81c7-4328-459f-944d-f55c52e31fb1/

Morgus, R., Skierka, I., Hohmann, M., Maurer, T. (2015a), CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams, GPPi. Retrieved from: http://www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf

Morgus, R., Skierka, I., Hohmann, M., Maurer, T. (2015b), National CSIRTs and Their Role in Computer Security Incident Response, GPPi. Retrieved from: https://na-production.s3.amazonaws.com/documents/CSIRTs-incident-response.pdf

NCSC-NL (2015). CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity, NCSC-NL, The Hague, Netherlands, retrieved from: https://check.ncsc.nl/static/CSIRT_MK_guide.pdf

Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver M.H.A. (2008). "Modeling Critical Infrastructure Dependencies", in: IFIP Vol. 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, pp. 205-214.

Nippon CSIRT Association (NCA). Retrieved at http://www.nca.gr.jp/en/index.html

Open CSIRT Foundation (OCF). Retrieved at: https://www.opencsirt.org/

Organization of American States (2016). Best Practices for Establishing a National CSIRT / Buenas Prácticas para establecer un CSIRT nacional (versions in English and Spanish), General Secretariat of the Organization of American States (OAS), Washington DC, USA. Retrieved from: https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf [English] / https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf [Spanish]

Stikvoort, D. (2008). SIM3: Security Incident Management Maturity Model, Netherlands. Retrieved from: https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

Trusted Introducer Certification process (2009-today). Retrieved from: https://www.trusted-introducer.org/processes/certification.html

UN GGE: UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). A/70/174 Report on 17th session: Developments in the field of information and telecommunications in the context of international security. Retrieved from: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (multiple languages)

West-Brown, M.J., Stikvoort, D., Kossakowski, K-P., Killcrece, G., Ruefle, R., Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs), CERT CSIRT Development Team, Carnegie Mellon University, Pittsburgh, USA. Retrieved from: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

This document was drafted and developed in cooperation with TNO and M7 for the Global Conference on Cyberspace GCCS in India (2017). Many thanks to all others, especially those from CSIRT communities, who participated in the realisation of this document.

GFCE
Global Forum on Cyber Expertise