
Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers

March 2020

Contents

About this guidance document	01
Introduction	01
What is an NCSS?	02
Why involve stakeholders?	03
Who are the relevant stakeholders?	04
How to involve stakeholders	05
Stage 1: Initiation	05
Stage 2: Stocktaking and analysis	07
Stage 3: Production of the NCSS	09
Stage 4: Implementation	12
Stage 5: Monitoring and evaluation	13

About this guidance document

This report is designed to guide policymakers on how to develop, implement and review a National Cybersecurity Strategy (NCSS) with the active and ongoing involvement of relevant stakeholders. Other stakeholders may also find it useful when considering the roles they can play in this process.

Introduction

There is a growing recognition that fostering a cyberspace that is free, open and secure requires a multistakeholder approach to cybersecurity capacity building.

A National Cybersecurity Strategy (NCSS) lies at the core of these efforts. By providing a comprehensive framework for prevention, preparation, response, and incident recovery, the NCSS represents a critical element of a country's cybersecurity maturity and readiness. The measures taken to implement the NCSS—whether legislative, institutional, technical or otherwise—can help reduce the scale of cyberthreats and cyberattacks, as well as minimise their impact when they occur.

Cybersecurity, however, is not solely an issue for governments—, and ensuring a free, open and secure cyberspace is not the preserve of any single stakeholder group. As noted elsewhere, *“cybersecurity is a shared responsibility which requires coordinated action (...) on the part of government authorities, the private sector and civil society. For this to operate smoothly and to ensure a safe, secure and resilient digital realm a comprehensive framework or strategy is necessary, which has to be developed, implemented and executed in a multi-stakeholder approach.”*¹

How to effectively involve stakeholders in the process of developing, implementing and reviewing a country's NCSS is therefore a fundamental question for anyone interested in cybersecurity capacity building.

But while most agree on the value of an inclusive approach to cybersecurity, implementing it is not always straightforward. Facilitating meaningful stakeholder engagement requires dedicated effort and leadership, as well as a specialised set of skills and knowledge. Even in cases where these conditions are met, a lack of practical guidance continues to stifle roll-out and adoption.

This guide aims to address this by providing practical advice for policymakers and other stakeholders in their efforts to facilitate an inclusive approach to NCSS development, implementation or review. It sets out specific considerations for each stage of the NCSS lifecycle, outlines how relevant stakeholders may be identified, and suggests various modalities for their meaningful engagement, illustrated by real life examples sourced from research and GPD's engagement on the ground.

¹ International Telecommunication Union, *National Strategies*, available at: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx>.

What is an NCSS?

An NCSS is a framework which sets out the government’s approach toward cybersecurity, usually over a period of a few years. As well as setting out the government’s vision and objectives, and the principles that guide the strategy, NCSSs often also set out a series of actions, programmes or initiatives that should be implemented to help achieve their objectives.

The content of an NCSS varies from country to country. Some may include further sections, covering—for example—governance of the strategy, or baseline assessments of the existing cybersecurity landscape. There are already a number of guidance documents which set out what an NCSS should contain, such as the International Telecommunications Union’s (ITU) [Guide to Developing a National Cybersecurity Strategy](#), and the European Union Agency for Network and Information Security’s [National Cyber Security Strategy Good Practice Guide](#). This guidance document seeks to complement and build on these existing resources, by focusing more directly on how to involve stakeholders at different stages of the NCSS lifecycle.

The NCSS lifecycle

The NCSS lifecycle refers to the series of stages that form part of the process of developing and implementing an NCSS. The lifecycle may vary in practice, but setting it out offers a useful means of structuring the steps through which an NCSS is crafted and operationalised. For the purpose of this guidance document we have chosen to use the following lifecycle model:²

- Stage 1: Initiation
- Stage 2: Stocktaking and Analysis
- Stage 3: Production of the NCSS
- Stage 4: Implementation
- Stage 5: Monitoring and Evaluation

As its name suggests, the NCSS lifecycle is a process that should be continual and cyclical, rather than a one-off event. The cybersecurity landscape is evolving too fast to assume that a one-off strategy will be sufficient to ensure a nation’s cybersecurity posture is adequate to account for future threats and attacks. 💡

² As outlined in International Telecommunication Union (ITU), *Guide to Developing a National Cybersecurity Strategy*, November 2016, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

Why involve stakeholders?

As noted above, existing guidance documents on developing an NCSS all highlight the importance of engaging a wide range of relevant stakeholders in the process.³ While there is an intrinsic value to involving a wide range of stakeholders in cybersecurity processes, there are two practical reasons why engaging stakeholders into the NCSS process specifically is beneficial.

1) Better informed and evidence-based policy outcomes

Cybersecurity, as a question of public policy, affects a range of different stakeholders, many of whom have different experience and areas of expertise on the subject. Much of this is unlikely to exist within government alone. The private sector, for example, will have a unique understanding of the cyberthreats that businesses face, as well as the products and services being developed that can help increase cybersecurity. Civil society organisations may have particular expertise in the human rights implications of different policies under consideration, the specific cybersecurity threats faced by different groups within society, and experience in working directly with individuals to take steps to protect themselves online. Bringing this expertise into the NCSS process can help get a more accurate and evidence-based picture of the cybersecurity landscape, the possible implications of different policies being considered, and how best to engage with those other stakeholders during the NCSS's implementation and review stages.

2) More effective implementation of the NCSS

As noted above, the range of different stakeholders who are involved in efforts to increase a country's cyber maturity level means that their involvement in the implementation of any NCSS is inevitable. Indeed, almost all NCSSs contain sections on public-private partnerships, research and development funding, and public awareness-raising, all of which involve non-governmental stakeholders. Successful and effective implementation of an NCSS relies, in part, on ensuring that all relevant stakeholders have confidence and trust in the NCSS itself, as well as in the other stakeholders involved in its implementation. Stakeholders who have been involved in the development of the NCSS will have a stronger understanding of the strategy and what is required from them making implementation efforts more effective. And, when it comes to reviewing an NCSS, the feedback and information provided by various stakeholders is vital; and this feedback and information is much more likely to be forthcoming if those stakeholders have been part of the NCSS's development and implementation. This also helps to ensure that further iterations and revisions make the NCSS more effective.

³ See, for example: International Telecommunication Union, *Guide to Developing a National Cybersecurity Strategy*, November 2016, p.31; and Commonwealth Telecommunications Organisation, *Commonwealth approach for developing national cybersecurity strategies*", 2015, p. 12.

Who are the relevant stakeholders?

Different stakeholders may be involved in different ways and at different stages of the NCSS lifecycle. So how do we identify the relevant stakeholders?

Broadly speaking, all stakeholders are relevant when it comes to cybersecurity, because everyone has an interest in ensuring a free, open and secure cyberspace. But when it comes to cybersecurity policymaking more specifically, *relevant* stakeholders tend to refer to:

- Those with a mandate, role, or responsibility in the process;
- Those with skills or expertise needed to inform the policy and operationalise it, and
- Those who could be disproportionately affected by the policy or its implementation.

These stakeholders may belong to a range of stakeholder groups, including:⁴

- Different government departments, in particular those dealing with national security and resilience, defence, relevant infrastructure such as telecommunications and energy, information and communication technologies, and with foreign affairs;
- Other public bodies whose mandate also includes the above issues, such as telecommunications regulators;
- The judiciary and law enforcement;
- Academic institutions whose expertise includes cybersecurity, such as universities, research entities, think tanks, and independent experts and researchers;
- Civil society organisations, particularly those with expertise in human rights, those who engage with different groups and communities within society vulnerable to cyberattacks, those which engage directly with the public on cybersecurity-related issues, and networks and umbrella groups;
- International and regional organisations whose mandate or expertise includes cybersecurity, such as the ITU, the Organisation of American States or the World Bank;
- The technical community, including members of the incident response community, standard setting organisations, and domain name systems;
- The private sector, including trade associations, particularly those from industries and sectors that are particularly vulnerable to cyberthreats, or who develop technology or provide services that enhance cybersecurity.

When should relevant stakeholders be identified?

As well as conducting a comprehensive mapping of the stakeholder landscape at the beginning of the process (see page 6 below), it is also valuable to undertake specific assessments at each subsequent stage of the NCSS lifecycle.

Doing so may not only help identify the relevant stakeholders, but also, through speaking to them, help identify levels of their cybersecurity awareness and where additional skills and expertise may be needed.

⁴ Global Partners Digital, *Multistakeholder Approaches to National Cybersecurity Strategy Development*, June 2018, p.13.

Mapping stakeholders will be the first step, but it is not alone sufficient. It's important to develop a holistic engagement plan with clear rules of engagement throughout the process.

The government should engage as wide a range of stakeholders as possible, so as to ensure that key perspectives and critical expertise are not missed. In the rapidly evolving digital environment, as new risks and opportunities emerge, the approach to identifying relevant stakeholders should aim to be as inclusive, flexible, and “future-proof” as possible. 💡

How to involve stakeholders

Despite there being different ways in which stakeholders can be engaged throughout the lifecycle of the NCSS, the aim should be to engage stakeholders in a holistic, sustained way. Piecemeal multistakeholder approaches can only be partially successful. In other words, if relevant stakeholders are only invited to comment on the NCSS in the later stages of drafting, or—for example—are involved in the implementation of the NCSS but were not invited to engage in the development process, then the value of stakeholder engagement will not be as high as it could be.

Stage 1: Initiation

This stage focuses on securing political buy-in and strategic vision for the NCSS, establishing key structures and processes, and identifying relevant stakeholders.

Besides the general benefits of a multistakeholder approaches outlined above (p. 3), a multistakeholder approach to the initiation stage will be particularly useful— in facilitating access to stakeholder networks relevant for subsequent lifecycle stages, and helping build trust and stakeholder confidence in the overall process.

A key activity in this stage is **setting up the governance structure** which will guide and oversee the remaining stages of the NCSS lifecycle. The structure itself can take many forms, including a steering committee, a working group or task force.

Involvement of stakeholders can range from formal to informal, and from consultative—in which the government has the primary role, but consults other stakeholders, for example via a non-governmental advisory group—to that in which government and non-governmental stakeholders deliberate and make decisions on an equal footing.

Transparency and communication are key. At this stage it is crucial to share the roadmap for NCSS development with stakeholders, and to be clear on roles and responsibilities and rules of engagement. Doing this will ensure each stakeholder has clarity with regard to at which subsequent stages they'll be called upon, and how they'll be expected to contribute to the process following the initiation stage.

In Belize, the government established a **multistakeholder NCSS Task Force** under the leadership of the government's National Security Council Secretariat (NSCS) and with support of the Organization of American States Inter-American Committee against Terrorism (OAS/CICTE) Cyber Program⁵. The Task Force comprised 15 different entities, ranging from governmental stakeholders and the private sector to civil society and academia. It was formed in mid-2017, after the first National Cybersecurity Symposium, and started coordination for the development of the Strategy in 2018.

The Task Force held around ten different meetings throughout the process. In addition to leading on the drafting of the strategy, the Task Force played a key role in helping shape capacity building efforts led by the NSCS and GPD, which were aimed at building the capacity of non-governmental stakeholders to engage in the development of the strategy. The Task Force is still active and is expected to remain engaged in the NCSS implementation. 🔧

Since only a small number of stakeholders will likely be involved in the NCSS governance structure, involving non-governmental stakeholders complements and enhances, rather than substitutes for, the engagement of a broader range of stakeholders during the remaining stages. 💡

⁵ <https://mns.gov.bz/regional-security/belize-adopts-cyber-security-strategy/>

Stage 2: Stocktaking and analysis

This phase focuses on collecting the information needed to assess the existing national cybersecurity landscape so as to help inform the development and drafting of the NCSS (Stage 3). There are a number of independent assessment frameworks to help structure the exercise, including the Oxford Cybersecurity Capacity Maturity Model for Nations (CMM)⁶ and the ITU's Guide to Developing a National Cybersecurity Strategy.⁷ This exercise may be conducted by the NCSS lead authority or equivalent body, or contracted out to external bodies or experts.

Involving stakeholders at this stage will be key in helping ensure a well-informed and evidence-based approach to the NCSS. As noted earlier in this guide, while some information needed to inform the development of the NCSS will exist within government, much will not—but will instead be known by other stakeholders. This could include information on the cybersecurity threats and challenges that different stakeholders are concerned about, the products and services developed and offered by the private sector to address such threats and challenges, and existing capacity building efforts being undertaken by non-governmental stakeholders to build cyber resilience.

Engaging stakeholders at this stage also provides an opportunity to raise the awareness of stakeholders on key cybersecurity issues, and to build their capacity to engage in and support the later stages of the NCSS life cycle (such as implementation).

How can stakeholders be involved in this stage? One cost-efficient way of gathering stakeholder input can be through **online consultations or questionnaires**. These might be open to anyone or more targeted, asking specific questions of certain stakeholders and actors. Online consultations may be particularly useful in cases where bringing people together physically poses practical challenges or costs are prohibitive.

In 2016, the Inter-American Development Bank (IDB), the OAS, and the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford gathered data on the cybersecurity landscape of countries in Latin America and the Caribbean to inform the 2016 report entitled “Cybersecurity: Are we ready in Latin America and the Caribbean?”⁸

The data was collected through an online survey based on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the GCSCC and translated into English and Spanish. The online survey was administered to a wide cross-section of national stakeholders in 32 countries in Latin America and the Caribbean. The responses received were aggregated, reviewed, and

⁶ Available at: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0>

⁷ International Telecommunication Union, Guide to Developing a National Cybersecurity Strategy, November 2016, pp. 21-22.

⁸ <https://www.cybersecobservatory.com/2016/11/12/cybersecurity-ready-latin-america-caribbean/>

complemented with additional sources of information. The dataset was made available online.⁹

An alternative means to gather information is through **in-person meetings** or workshops. Again, these could be open to anyone, or closed—with invitations only to particular stakeholders and actors. In either case, in-person meetings may look at the full range of issues on which information is sought, or focus on particular themes. In-person meetings have the benefit of allowing dialogue between different participants, which is not feasible in an online consultation.

This exercise of gathering information on the overall cybersecurity landscape can also help identify priorities which will inform the production of the NCSS itself (i.e. the first part of Stage 3).

Sierra Leone is in the process of developing its national cybersecurity strategy, under the leadership of the Ministry of Information and Communication. As part of this process, the Ministry convened a **multistakeholder workshop** with the aim of increasing awareness among stakeholders with regard to cyber policy issues, gathering information on the landscape, increasing coordination, and providing a space for stakeholders to discuss their priorities and inform the process of NCSS development.¹⁰

In addition to that stakeholder workshop, the Ministry subsequently co-convened a civil society training workshop to build capacity of civil society groups to enable them to engage in cyber policy discussions, and the NCSS development process in particular.¹¹

In Ghana, a cybersecurity capacity maturity review was undertaken by the GCSCC using Oxford's Cybersecurity Maturity Model (CMM).¹² The assessment was undertaken through **closed in-person meetings and workshops** with the aim of gaining a more in-depth understanding of Ghana's cybersecurity capacity, and identifying areas for further investment. The meetings were attended by various local and international stakeholders. Engagement of stakeholders during this stage was singled out as an important factor in getting an accurate picture of the Ghanaian cybersecurity landscape. Besides informing the CMM, engaging stakeholders at this stage also led to greater stakeholder engagement in the NCSS drafting process that followed.

⁹ <https://mydata.iadb.org/Reform-Modernization-of-the-State/2016-Cybersecurity-Report-Data-Set/cd6z-sjjc>

¹⁰ <https://awokonewspaper.com/sierra-leone-news-matthew-shears-global-digital-partners/>

¹¹ <https://www.facebook.com/acdro2/videos/2477159255939288/>

¹² <https://www.moc.gov.gh/cybersecurity-capacity-maturity-model-assessment-held>

Stage 3: Production of the NCSS

This phase focuses on the development of the text of the NCSS itself, from initial planning around what the NCSS will contain, to the text's drafting, review and validation. The exercise will ordinarily be led by the governance structure set up in Stage 1 of the lifecycle (although external actors, such as consultants, may also be involved) and should take into consideration the results of the stocktaking and analysis conducted at Stage 2.

By bringing in the additional expertise and knowledge that exists among different stakeholders, the text of the NCSS itself is likely to be more evidence-based and therefore more likely to be effective. Engaging stakeholders and taking into account their feedback and perspectives will also strengthen trust and confidence among those stakeholders in both the NCSS itself, and the process of its development. Given that many of these stakeholders will be involved in the implementation of the NCSS, greater trust and confidence will likely ensure more effective implementation.


Stakeholders can be engaged at all points of the production of the NCSS. To start with, stakeholders should be drawn upon to inform the **structure, objectives and priority areas** for the NCSS. Here, modalities for gathering information will be the same as those employed in Stage 2, or some combination of the above. This is a critical opportunity to get stakeholder input and identify priorities that the strategy should address.

✎ The Australian Government is currently working on a new NCSS. As part of the strategy development, a series of **open forums** was convened in different cities across the country, as well as an initial **open online consultation** which aimed to inform the strategy's development. The government published a cybersecurity strategy discussion paper and requested contributions from stakeholders. The paper outlined some guiding questions on specific cybersecurity topics, as well as a more open question for further consideration. The call for comments was open for three months and gathered a total of 213 submissions. Public submissions were posted on the website of Australia's Home Affairs¹³, making the process open and transparent.


✎ The Government of India is currently working on the development of their National Cybersecurity Strategy, the successor their 2013 National Cyber Security Policy. To ensure broad stakeholder input, they launched a public **online consultation** to seek input on the vision and pillars of the upcoming strategy. The public consultation was open for two months.¹⁴

¹³ <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020>


¹⁴ <https://ncss2020.nic.in/>


In Papua New Guinea, back in 2017, the National Information and Communications Technology Authority invited stakeholders to provide written inputs via an **online questionnaire** to inform the development of Papua New Guinea's first national cybersecurity strategy.¹⁵ 

Who holds the pen? The **drafting of the text** is likely to be led by the lead authority or governance body set up in Stage 1 (although it could also involve an external actor, such as a consultant). As noted above, this structure can itself be multistakeholder, ensuring a more inclusive approach to the drafting process.

As explained in one of the previous examples, a **multistakeholder NCSS Task Force** was set up in Belize to lead on the development of the NCSS. It was formed at the beginning of the NCSS development process in mid-2018 and led on the drafting of the strategy, with the support of the OAS/CICTE Cyber Program. 

Once a draft NCSS is ready, stakeholders can be invited to **review and comment on the text** through consultation—whether online or in person. At this point, and depending on the feedback received, further iterations of drafting and review may need to be undertaken, at least in respect of certain parts of the NCSS.

In Belize, once a first draft was developed by the dedicated multistakeholder task force, an **open online consultation** was undertaken by the Government with the aim to gather stakeholder feedback on the text. The text of the first draft was published online on the Belize Crime Observatory Website¹⁶, the Government body that led the process of developing Belize's first NCSS. The draft was open for comments, suggestions and edits from stakeholders for three weeks. In addition to this, the government shared the strategy draft via email, inviting specific stakeholders to input. Having the opportunity to provide input online made the process more accessible to those stakeholders unable to participate in in-person consultations, thus making the process more inclusive. 

Kenya adopted its first National Cybersecurity Strategy in 2014. During the development of the strategy, the Government conducted a **closed online consultation** when a draft of the NCSS was shared with the KICTANet list (a multistakeholder mailing list), reaching a broad range of stakeholders. 

Finally, although the adoption of the NCSS will be reserved for the designated government body, validation of the NCSS involving a broader range of stakeholders before moving to formal adoption can be an effective way to build

¹⁵ <https://www.nicta.gov.pg/2017/08/gpn-0-7/>

¹⁶ <https://bco.gov.bz/download/belize-national-cyber-security-strategy-dec-2019-draft/>

trust and ensure stakeholder buy in. Holding a validation workshop at this stage of the process is strongly encouraged.

In Ghana, a **validation workshop** was held before adopting the first Ghanaian National Cybersecurity Policy and Strategy (NCPS) in 2015. It gathered representatives from different stakeholder groups to discuss the need for a detailed implementation framework, in order to help the NCPS serve as a road map to address cyber threats. This final moment of assent from stakeholders was seen as essential to ensure broader community buy-in, and to the legitimacy of the development process itself. Since then, Ghana has reviewed its National Cybersecurity Policy and Strategy under the leadership of the National Cybersecurity Centre, convening an open forum where the revised draft was presented for stakeholder input and validation. 🛠️

Stage 4: Implementation

Stage 4 focuses, as its name suggests, on implementing the NCSS which was produced during Stage 3. This means identifying and then implementing concrete actions set out in the NCSS and any accompanying Action Plans—such as setting up emergency response teams, building cyber hygiene awareness programmes, and protecting critical infrastructure. The precise roles and responsibilities of different stakeholder groups in relation to these actions should have been determined during the production of the NCSS.

There are two elements to this stage:

1. The development of the Action Plan (which identifies the implementation actions);
2. The implementation of those actions.

The **development of the Action Plan** can happen after the production of the NCSS (Stage 3) or in parallel. In either case, it should use the same modalities by which stakeholders were engaged during Stage 3.

At this point, it might be worth considering whether—regardless of the overall NCSS governance structure established at Stage 1—additional multistakeholder mechanisms should be established, such as task forces or working groups, to coordinate, oversee or implement the Action Plan or specific activities.

When it comes to **implementing actions**, given the range of activities at hand, different stakeholders might need to be involved in different activities to ensure effectiveness. Some actions—such as efforts to protect critical information infrastructure—are highly reliant on private sector and technical community engagement, while others—such as building educational and awareness programs—won't be implementable without civil society support.

Depending on the existing interest and capacity of local stakeholders, additional investment and efforts might be necessary to facilitate meaningful stakeholder engagement at this stage. As noted above, earlier stages of the NCSS lifecycle, particularly Stage 2, are important opportunities to gauge stakeholder interest and capacity.

In June 2018, Vanuatu launched its national Computer Emergency Response Team, CERT VU, in line with its 2013 National Cybersecurity Policy. CERT VU aims to enhance and strengthen Vanuatu's national security, and was formed as a result of a collaborative multistakeholder process supported by a **working group comprised of 12 local actors**, as well as Asia Pacific Network Information Centre (APNIC)¹⁷. They were reported to be encouraged by the successful establishment of Tonga's CERT in 2016, finding the multistakeholder model relevant to their situation. A case study by APNIC on the formation of CERT VU highlighted how the engagement of several stakeholders helped build momentum behind the set-up of the CERT. 🛠️


¹⁷ <https://blog.apnic.net/2019/04/23/the-road-to-a-national-cert-in-vanuatu/>

Stage 5: Monitoring and evaluation

Stage 5 focuses on the development of a process to monitor and evaluate the NCSS and its implementation. Part of this stage may need to take place in parallel with Stages 2, 3 and 4—particularly the development of a process and framework to monitor the NCSS’s implementation. This evaluation of the NCSS should, however, take place at the conclusion of the NCSS’s lifespan. The results of any monitoring and evaluation should also feed into Stage 2 of the next iteration of the NCSS lifecycle, as part of the stocktaking and analysis.

At this stage, stakeholders should be able to provide information necessary to evaluate the overall success of the NCSS and the extent to which it has met its goals and objectives. They could also help identify whether any revisions are needed—for example, to respond to new cyberthreats—and identify lessons learned.

The modalities for engagement by stakeholders will mirror those outlined above, particularly at Stage 2 (e.g. online consultations or in-person meetings and workshops).

In Botswana, a **workshop** with stakeholders was convened in early 2019 to review the implementation of its NCSS, which was developed by the government in partnership with the private sector, and to discuss cybersecurity priorities, challenges, and a roadmap for the year ahead.¹⁸ 

¹⁸ <http://www.botswanaguardian.co.bw/news/item/3945-cyber-security-stakeholders-introspect.html>

GLOBAL PARTNERS DIGITAL

Second Home
68 Hanbury St
London E1 5JL

+44 203 818 3258