الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

RFC 2350

National Cybersecurity Authority (NCA)

1. Document Information

This document contains a description of NCA in according to RFC 2350.
It provides basic information about the National Cybersecurity Authority (NCA), its channels of communication, its roles and responsibilities and the services provided.

1.1. Date of Last Update

Version 1.0, Created 08-06-2020
Version 5.0, Modified 17-09-2024

1.2. Distribution List for Notifications

By subscribing to NCA (SeucirtyAlerts) mailing list, users receive information about vulnerabilities and its mitigations along with a weekly newsletter that contains the latest security alerts.
You can subscribe by visiting the link: https://nca.gov.sa/ar/newsletter/

1.3. Locations where this Document May Be Found

A current version of this RFC 2350 document is available on the National Cybersecurity Authority (NCA) website: https://nca.gov.sa/en/cyber-operations/

1.4. Authenticating this Document

This document has been signed with NCA InfoShare's PGP key.

2. Contact Information

2.1. Name of the Team

Full Name: National Cybersecurity Authority (NCA)
Short Name: NCA

2.2. Address

National Cybersecurity Authority
Al Raidah Digital City - An Nakheel District
Al Mahir Street, Building No 6672, Unit No. 3
Riyadh 12382 - 4149
Kingdom of Saudi Arabia

2.3. Time Zone

GMT+3

2.4. Telephone Number

We're available 24/7 on 800-124-9996

2.5. Facsimile Number

None

2.6. Other Telecommunication

None

2.7. Electronic Mail Address

info@nca.gov.sa
InfoShare@nca.gov.sa

2.8. Public Keys and Encryption Information

InfoShare
Fingerprint: 7AE2 DA28 E16A 9631 8853 9E3B 1C56 7A75 12DD 8970
https://nca.gov.sa/en/cyber-operations/

2.9. Team Members

The team leader, the general manager of the team and a full list of team members are not publicly available.
Management and supervision are provided by the Cybersecurity Technologies and Operations Sector, National Cybersecurity Authority (NCA).

2.10. Other Information

None

2.11. Points of Customer Contact

- For operational inquiries: https://haseen.gov.sa/form?id=f5d1894c-cd47-4024-b3c7-1ecf61894d46
- For general inquiries: info@nca.gov.sa and InfoShare@nca.gov.sa

3. Charter

3.1. Mission Statement

NCA's primary mission is to strengthen cybersecurity in the Kingdom to mitigate risks, boost trust, and enable growth.

The National Cybersecurity Authority (NCA) was established in 2017 by The Royal Order that links it directly to His Majesty, King Salman bin Abdulaziz Al Saud, to be the national authority in charge of cybersecurity in the Kingdom, and the national reference in all its affairs.

NCA aims at strengthening cybersecurity to safeguard the State's vital interests, national security, critical infrastructures, priority sectors, and government services and activities. However, without prejudice to the NCA's powers and duties provided for in its statute, public and private entities and any other entity shall not be relieved from their responsibility towards their own cybersecurity.

NCA's statute defines cybersecurity as "The protection of networks, information technology systems, and operational technology systems, including hardware and software, services provided thereby, and data included therein, against hacking, disruption, modification, unauthorized access, and unlawful exploitation or use. Cybersecurity includes information security, electronic security, digital security, and the like".

3.2. Constituency

The constituency of NCA is composed of everyone is the kingdom; public and private sectors and the general public.
National CSIRTs located outside of Saudi Arabia, services may be provided to any of these entities as requested, depending on resource availability.

3.3. Sponsorship and/or Affiliation

Member of FIRST
Member of Trusted Introducer (TI)
Member of OIC CERT

3.4. Authority

The National Cybersecurity Authority (NCA) is the government entity in charge of cybersecurity in Saudi Arabia, encompassing both regulatory and operational functions related to cybersecurity.

4. Policies

4.1. Types of Incidents and Level of Support

NCA works as coordinator for mitigating the impacts of security incidents at an appropriate support level depending on the type, severity and extent of the incidents.

4.2. Co-operation, Interaction and Disclosure of Information

NCA classifies data and information in all forms. It intends to set the appropriate classification levels to apply the corresponding security measures and reduce the risk of protected information disclosure.

NCA classifies its information based on the information sensitivity and impact on its business. There are four classification levels (Top Secret, Secret, Restricted, Public). All incoming information received by NCA is being classified as per the sender's (Whether sent by an entity inside the kingdom or by an external/international entity) classification level according to applicable regulations and international agreements. However, if the incoming information is not being classified, the default applied classification is "Restricted".

4.3. Communication and Authentication

The preferred method of communication is via e-mail. When the content is sensitive enough or requires authentication, NCA's PGP key is used for signing. All sensitive communication to NCA shall be encrypted using the PGP key.

5. Services

NCA's Powers and Duties

- Drafting the national strategy for cybersecurity, supervising its implementation, and proposing updates thereto.
- Setting cybersecurity policies, governance rules, frameworks, rules, standards, and directives; communicating the same to relevant agencies; monitoring compliance therewith; and updating them.
- Identifying and classifying critical infrastructures as well as the agencies related thereto, and identifying priority sectors.
- Setting and updating framework for cybersecurity risk management and monitoring compliance therewith.
- Notifying relevant agencies of cybersecurity risks and threats.

- Setting and updating frameworks for responding to cybersecurity incidents and monitoring compliance therewith.

- Establishing, supervising, and operating national cybersecurity operation centers, and the like, including centers for control, surveillance, monitoring, exchange, and information analysis; sectoral cybersecurity operation centers, as necessary; and relevant platforms.

- Conducting, on its own or through others, cybersecurity activities and operations.

- Regulating and supervising the sharing of cybersecurity-related information and data between various agencies and sectors in the Kingdom.

- Providing support to relevant agencies, upon request and in accordance with the NCA's available resources, during the investigation of cybersecurity crimes.

- Setting and updating national encryption policies and standards and monitoring compliance therewith.

- Setting and updating standards for licensing the import, export, and use of highly sensitive cybersecurity hardware and software specified by the NCA and monitoring compliance therewith, without prejudice to the standards or requirements of other relevant agencies.

- Building national capacities in cybersecurity, participating in the preparation of educational and training programs, setting professional standards and frameworks, and developing and implementing relevant professional standardized tests and measurements.

- Licensing individuals and non-government agencies to engage in cybersecurity activities and operations specified by the NCA.

- Establishing ties with counterpart agencies abroad and private entities to exchange expertise and establish frameworks for cooperation and partnership, in accordance with applicable procedures.

- Exchanging technological and informational production as well as data and information with counterpart agencies aboard.

- Representing the Kingdom in relevant regional and international organizations, agencies, and bilateral committees and groups as well as monitoring the Kingdom's compliance with its international cybersecurity obligations.
- Raising awareness on cybersecurity.
- Stimulating the growth of the cybersecurity sector in the Kingdom and encouraging innovation and investment therein.
- Conducting research and development studies, carrying out manufacturing processes, and transferring and developing technology in cybersecurity and related fields.
- Proposing mechanisms to optimize spending pertaining to cybersecurity.
- Developing key performance indicators relating to cybersecurity and preparing periodic reports on the state of cybersecurity in the Kingdom at the national and sectoral levels.
- Proposing cybersecurity laws, regulations, and decisions as well as amendments.

6. Incident Reporting Forms

To report an incident or vulnerability to NCA, please visit:

- https://haseen.gov.sa/form?id=f5d1894c-cd47-4024-b3c7-1ecf61894d46

7. Disclaimers

The information in this document are provided on a "as is" basis. The National Cybersecurity Authority (NCA) does not guarantee the accuracy, adequacy or completeness of this information.

The National Cybersecurity Authority (NCA) expressly disclaims liability for any damage caused by error or inaccuracy in the information or any decision based on the information contained in this document.