UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

CYBER SECURITY INFORMATION SHARING FRAMEWORK

May 2023

Version 1.0

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.

VERSION CONTROL

Version	0.1
Date:	12 May 2022
Prepared by:	CSC
Amendment Content:	Initial Draft Document

Version	0.2
Date:	25 June 2022
Prepared by:	CSC
Amendment Content:	Updated based on initial feedback

Version	1.03
Date:	30 August 2022
Prepared by:	CSC
Amendment Content:	Updates as per review comments on the draft v0.2 of the document

	Reviewed by	Approved by
Designation:	xxxxxxxxx	xxxxxxxxx
Name:	xxxxxxxxx	xxxxxxxxx
Signature:	xxxxxxxxx	xxxxxxxxx
Date:	xxxxxxxxx	xxxxxxxxx

Table of Contents

SECTION 1

INTRODUCTION

INTRODUCTION

The increased connectivity of cyberspace has led to significant transformations, economies of scale and efficiencies across the UAE - and around the world. It has also increased the complexity of our shared cybersecurity threats. As a global leader in ICT adoption, the UAE confronts a dangerous combination of known and unknown vulnerabilities in cyberspace. In addition, threats (natural and man-made, deliberate, and unintentional) are rapidly becoming more diverse and capable, increasing both the frequency, sophistication, magnitude, and consequences of cybersecurity incidents.

There is a growing awareness of cybersecurity risk and its implications for national and international security. The sharing or exchange of cybersecurity information is therefore seen as an increasingly critical component in reducing cybersecurity risks across the UAE government and Critical Information Infrastructure (CII).

The Council has developed this framework to establish a National Cybersecurity Information Sharing Framework to promote and institutionalize cybersecurity information sharing and collaboration across multiple stakeholders. This framework is aligned with the UAE’s national priority to be a global leader in cyber security and will enhance the security posture of organizations and individuals across the UAE.

1.1 Purpose

The National Cybersecurity Information Sharing Framework describes a consistent and repeatable means of conveying cybersecurity information or experience from one trusted party to another. Further, it also includes the descriptions and types of information for key threat information-sharing entities. The framework will enhance collaboration amongst stakeholders in the UAE cyberspace, building trust across the ecosystem and reducing cybersecurity risk at a local, regional, national and global level.

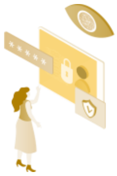
The framework sets out to promote timely and secure exchange of cybersecurity information such as risks, threats, vulnerabilities, countermeasures, best practices and lessons learned. Additionally, it focuses on promoting a decentralized, distributed, and coordinated environment enabling stakeholders across a diverse ecosystem to exchange cybersecurity information to strengthen the security and resilience of the UAE's cyberspace. It builds on existing practices and outlines the best practices for new information sharing capabilities for the UAE.

1.2 Scope & Applicability

The cybersecurity information sharing ecosystem covers a broad range of stakeholders, from national level entities through to individual citizens of the UAE. The framework addresses key cybersecurity functions at the national, emirate and sector level and across the various stakeholder groups and interested parties. The extent of applicability is as follows:

National Level Entities

The framework lays out foundational elements for interaction among federal entities that have responsibility for national cybersecurity and resilience.



Emirate Level Entities

The framework outlines the role of individual Emirates, and their lead entities, in governing and regulating cybersecurity information sharing within their specific Emirate.

Critical Information Infrastructure Sectors

The framework outlines the role of individual sectors, and their lead entities, in governing and regulating cybersecurity information sharing within their specific sector.

Other entities

The framework will serve as a guideline to all entities (non-CII entities, startups, academia, and service providers) operating in the UAE to participate in good governance for cybersecurity in the UAE.

General populace

The framework will serve as reference to understand cybersecurity information sharing practices in the UAE and their individual role within the UAE ecosystem of stakeholders.

International Partners

The framework will serve as a reference to understand cybersecurity information sharing best practices in the UAE and how they can best engage with the UAE ecosystem of stakeholders in cybersecurity information sharing.

1.3 Guiding Principles

The framework is built on the basic tenants described below to ensure a holistic and efficient information sharing ecosystem in the UAE.

Build ecosystem of trust

Foster confidence that information provided will be acted upon and that it will be protected and/or shared appropriately within information sharing communities.

Common language

Build standardized data formats and information sharing protocols enabling automation and allowing organizations to exchange information thus encouraging interoperability

Compliance to laws and regulations

Account for legal and regulatory mandates when sharing information to ensure compliance and to protect against breach of sensitive information for all participating entities.

Shared situational awareness

Leverage the collective knowledge, experience, and analytic capabilities thereby enhancing defensive capabilities of multiple organizations participating within a community.

SECTION 2

CYBER SECURITY INFORMATION SHARING FRAMEWORK

The Cybersecurity Information Sharing Framework has been established to enable near real-time sharing of cybersecurity information and ideas among the stakeholders who play a role in protecting and enhancing the resiliency of the UAE's cyberspace. Collectively, this environment will promote cyber security awareness, enhance resiliency and preparedness, enable effective and timely cyber incident response, and support continued innovation and growth.

This framework will enable entities to understand:

- Why cybersecurity information needs to be shared (i.e., value proposition),
- What cybersecurity information needs to be shared (i.e., types of information),
- Who needs to share cybersecurity information (i.e., participating stakeholders), and
- How should the information be shared (i.e., platform for sharing).

2.1 Cyber Security Information Sharing Framework Overview

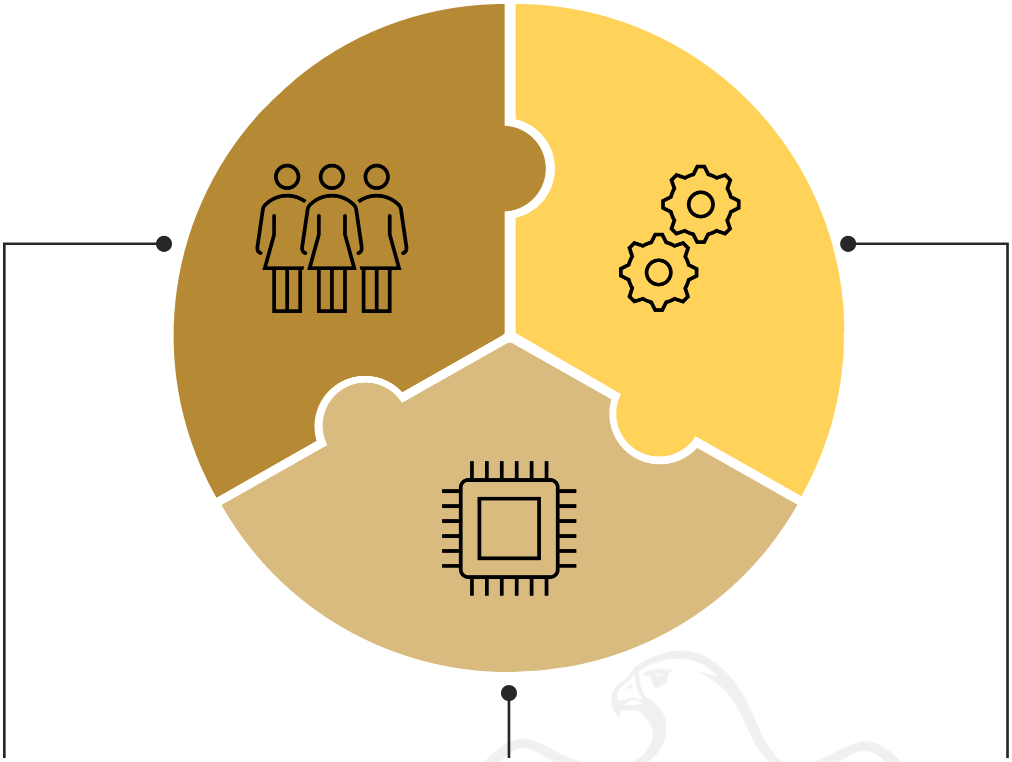
To build a decentralized, distributed, and coordinated environment, enabling individuals across a diverse stakeholder community to exchange information, the integration of people, process, and technology is necessary.

- **People:** The governance and working group mechanisms to enable trusted relationship building and inform rapid, structured, and distributed decision-making necessary to protect cyberspace.
- **Process:** The rules for sharing, including defining the rules of engagement (i.e., non-disclosure agreements (NDA), information sharing access agreements (ISAA), governance charters for information sharing working groups, etc.), standards, and roles of stakeholders internal and external to the participating organization; and
- **Technology:** The tools, systems, and protocols that provide the secure platform to enable the flexible sharing of timely information and that address the safeguarding of critical information.

2.1 Information Sharing Framework Overview

The framework therefore comprises of the following six core elements across People, Process and Technology:

Information Sharing Framework Elements



People

- Stakeholder
- Information sharing community

Technology

- Mechanism of information exchange

Process

- Types of information
- Models of information exchange
- Methods of information exchange

2.2 Information Sharing Framework Elements

People

2.2.1 Stakeholders

The individuals or types of organizations, each with their own perspectives, interests, and needs, greatly influence the formation of any information exchange. These stakeholders may also have varying degrees of technical capability, face significantly different threats, and have separate motivations for acting upon cybersecurity information.

The following are the stakeholders and their roles in the cybersecurity information sharing ecosystem:

National Level Entities

These entities have the national economic and security duties that include the need to defend their own classified and unclassified systems/information, fight cybercrime, and help reduce the cybersecurity risk to the UAE citizens, residents, and visitors.

Emirate Level Entities

These entities define Emirate specific regulatory directives in line with UAE’s cybersecurity laws, and work closely with national entities to provide specialized security advice to entities dealing with cybersecurity security incidents and circulate proactive preliminary advisories.

Entities like the Abu Dhabi Digital Authority (ADDA) and Dubai Electronic Security Center (DESC), provide threat information to other entities within the Emirates.

Critical information infrastructure

Critical information infrastructure (CII) sectors and underlying entities need to share information on vulnerabilities, threats and best practices within sector as well as across sectors to support in building a national risk profile.

2.2 Information Sharing Framework Elements

People

2.2.1 Stakeholders

Other Entities

Private enterprises

Private companies have an interest in preserving the security of sensitive information, such as customer data, trade secrets, contract information, personally identifiably information and other intellectual property.

IT companies

Firms creating IT products and services have an interest in preserving the security and integrity of their offerings. They share information on vulnerabilities in products or services so that security firms can create solutions to remedy them, or they may produce and distribute software updates that remedy vulnerabilities for their customers.

IT Security Firms

IT security firms, including antivirus vendors, computer forensics experts, and penetration testers, collect and sell cybersecurity information, along with services flowing from that information, to other entities in the ecosystem.

General Populace

Security Researchers

Security researchers track malicious software and targeted attack campaigns, and they find vulnerabilities in software, hardware, and services through academic work, business, or voluntary collaborative efforts or to satisfy individual curiosity. They may notify relevant responders to help mitigate threats and remedy weaknesses, or they may choose to report their findings publicly.

2.2 Information Sharing Framework Elements

People

2.2.2 Cyber Security Information Sharing Communities

The scope of information exchange can vary from small, regional groups of researchers holding regular meetings and calls to discuss threats and vulnerabilities to high-level intelligence sharing between national governments.

The right actors are therefore critical to creating information exchange groupings. Information exchange is often composed of a community of individuals and organizations selected for their expertise, ability to effect change, and insight.

Cybersecurity Information sharing communities are established within the UAE, considering the scope and operational purpose for cybersecurity information sharing. The following are some of the types of communities:

Geographic Scope

International Cyber Security Information Sharing Communities: Cyber-threats are often international in scope. It is therefore important to enable information exchange participants to share information across borders. Entities participate in international cybersecurity information sharing forums/groups/communities to gain valuable insights and can share information depending on the type of information being shared, the sensitivity of the information and method of exchange. Dedicated members from National and or even CII Sector and Emirate Leads may be identified and nominated to participate in such International forums.

Regional Cyber Security Information Sharing Communities: Such communities promote information exchange programs allowing public and private sector entities, local companies, universities, and experts to come together and discuss threats and vulnerabilities within the middle east region.

National Cyber Security Information Sharing Communities: The inherent regulatory and security role of Cybersecurity Council and various National level entities indicates the need for national information exchange programs. Numerous exchange programs at the national level have been established, both for voluntary and mandatory information exchange, covering all the major exchange stakeholders.

2.2 Information Sharing Framework Elements

People

2.2.2 Cyber Security Information Sharing Communities

Operational Purpose

Sector Specific Cyber Security Information Sharing Communities: Given the potential for threats within a single sector, sector-specific sharing has become a means of information exchange for critical infrastructure entities within a single sector.

Cross Sector Cyber Security Information Sharing Communities: Communities that bring entities from multiple sectors together to promote collaborative and cooperative information exchange using resilient and reliable resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats.

Common Interest Driven Cyber Security Information Sharing Communities: Communities that brings together a number of stakeholders, including private participants to exchange information regarding best practice followed or information on procedures for responding to security incidents.

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.1 Types of Information

Nine major types of information are typically shared through information exchanges. The following section illustrates how they relate to one another and how they can be leveraged for specific outcomes.

Strategic analysis

Gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks. This information is based on a variety of perspectives from incidents, proofs of concept, doctrines, and risk assessments and may be shared based on need-to-know basis.

Best practices

Information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics. Entities may choose to share this information in closed cybersecurity information sharing communities or publicly.

Situational awareness

Information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks. This type of data is often derived from vulnerabilities, incidents, mitigations, threats etc. and may be shared with all.

Incidents

Details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation. This information may be shared in closed cybersecurity information sharing communities, with regulators as required or with other entities that may be targets of similar attacks.

Vulnerabilities

Vulnerabilities in software, hardware, or business processes that can be exploited for malicious purposes. Vulnerabilities in software programs that need immediate patching will also be essential information to share, along with common attack patterns. Entities may choose to share this information in closed cybersecurity information sharing communities or publicly.

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.1 Types of Information

Mitigations

Methods for remedying vulnerabilities, containing, or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks. Entities may choose to share this information in closed cybersecurity information sharing communities or publicly.

Tactics, Techniques, and Procedures

Tactics, Techniques, and Procedures (TTPs) is a key concept in cybersecurity and threat intelligence. This will help entities identify patterns of behavior which can be used to defend against specific strategies and threat vectors used by malicious actors. Entities may choose to share this information in closed cybersecurity information sharing communities or publicly.

Threats

Threat information can help operators and entities detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others. Threats may be considered as yet-to-be-understood issues with potentially serious implications. Entities may choose to share this information in closed cybersecurity information sharing communities or publicly.

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.1 Types of Information

Indicators of Compromise

Indicators of Compromise (IOCs) are pieces of forensic data, such as data found in system log entries or files, which can help operators and entities identify potentially malicious activity on a system or network, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples or information about threat actors. At a minimum the following IOCs are monitored:

- Log-In Red Flags
- Increases in Database Read Volume
- Unusual DNS Requests
- Unexpected Patching of Systems
- Mobile Device Profile Changes
- Bundles of Data in the Wrong Place
- Web Traffic with Unhuman Behavior
- Signs of DDoS Activity
- HTML Response Sizes
- Large Numbers of Requests for the Same File
- Mismatched Port-Application Traffic
- Unusual Outbound Network Traffic
- Anomalies in Privileged User Account Activity
- Geographical Irregularities
- Suspicious Registry or System File Changes

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.2 Models of Information Exchange

Cybersecurity Information sharing can range from ad hoc exchanges to exchanges established through long-term formal structures. The different approaches most often reflect variables such as the level of trust between the parties, the legal authority of various actors, and the relationships between the stakeholders. Each model has its advantages but selecting the right model for the right purpose is vital to success. The following section highlights two exchange models: Voluntary sharing and Mandatory disclosure.

Voluntary exchange models

The Cyber Security Council encourages CII entities and private sector entities to voluntary exchange data and considers it to be the most valuable exchange that exists in the cybersecurity ecosystem. The voluntary cybersecurity information sharing allows actors to identify a need or a reason to exchange data and to begin to share and use what is valuable and actionable.

Entities decide with whom to share information based on the type of information involved and the purpose for cybersecurity information sharing either on a bilateral basis or may involve a group of entities.

Factors leading to voluntary information exchange may include, but not limited to:

- Contribution to a collective national defense or response.
- Protection of customers, brand, reputation, and products.
- Informing authorities of serious situations/incidents/potential threats.
- Reporting cybersecurity frauds or criminal activity.

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.2 Models of Information Exchange

Mandatory disclosure models

The disclosure of security event information to regulators and government authorities, investors, or impacted individuals, including customers. Types of information mandatory to be shared with Cyber Security Council may include but not limited to: Incidents, vulnerabilities, threats, and IOCs.

Mandatory information disclosure is inherently one-directional, focused not only on reporting itself but also how the gathered information will be used. Mandatory cybersecurity information sharing is scoped to ensure reported data is used to improve overall security and privacy within the nation.

Mandatory information disclosure models therefore consider:

- Clearly defined outcomes, such as protecting privacy, public safety, response coordination, or improving security defenses.
- Balance the risks and benefits associated with publishing incident details.
- Flexible and accepted approaches for sharing information as per defined timeframe.

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.3 Methods of Information Exchange

All cybersecurity information sharing communities identify the types of information they will be sharing and the circumstances under which they will be shared, and exactly who they will be sharing this information with. The methods of information exchange may be manual or automated. Methods of information exchange adopted within the UAE are as follow:

Formalized exchanges

The exchange of information is governed through service level agreements (SLAs), NDAs, and other agreements that describe the responsibilities of cybersecurity information sharing community members and participating organizations. Formalized information exchange may also include requirements of mandatory information disclosure to regulators and government authorities, or impacted individuals, based on National Policies and Frameworks.

Security clearance-based exchanges

A security clearance-based exchange represents a subset of a formalized exchange, one that is narrower in scope and participation. The information-exchange programs, especially those involving intelligence services, need to exchange classified and other sensitive information through protected channels, sometimes directly with a single party.

Ad-hoc exchanges

No formal agreements are required. Within the cybersecurity information sharing communities’ entities publish threat information on a voluntary, ad hoc basis and are individually responsible for ensuring that the content provided is suitable for sharing.

Trust-based exchanges

Trust-based groups are closed groups of like-minded cybersecurity actors who inform one another on an ad hoc basis when they see security issues of common concern. There are no formal agreements or contracts covering the exchange of information between members, but they may implement systems like the Traffic Light Protocol (TLP).

2.2 Cyber Security Information Sharing Framework Elements

Process

2.2.3 Methods of Information Exchange

Trusted Automated exchange of Intelligence Information (TAXII)

TAXII is the preferred method of exchanging information represented using the Structured Threat Information Expression (STIX) language, enabling organizations to share structured cyber threat information in a secure and automated manner.

Traffic Light Protocol

Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the appropriate audience. The TLP uses a color-coded system to identify those with whom information may be shared, thus signaling originator’s intent and easing fears about the extent of disclosure. The TLP also speeds information exchange since recipients intrinsically know with whom they can share that information without having to refer to the originator for permission to share it. Refer to Appendices.

2.2 Cyber Security Information Sharing Framework Elements

Technology

2.2.4 Mechanism of Information Exchange

An information exchange may use multiple mechanisms, depending on the nature of the information, actors involved, and the issues being addressed. To identify the most appropriate mechanism, the levels of automation required, and the format of the information being exchanged need to be considered.

Person to Person

The primary, and most effective mechanism of exchange is person to person (face to face or via web conferencing). These are often informal mechanisms of exchange, occurring during informal conversations. The cybersecurity information sharing community need to have encrypted channels of communication prepared for these vital mechanisms of exchange.

Machine to Machine

The use of automated exchange mechanisms helps reduce human resource costs and allow organizations to exchange threat information on a larger scale. An automated, machine-readable feed of threat and security information can be created using industry specifications, such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). Thus, information can be shared across industries and groups in near real time.

Structured Threat Information expression (STIX)

Structured Threat Information expression (STIX) - is a standardized language developed by MITRE and the OASIS Cyber Threat Intelligence (CTI) Technical Committee for describing cyber threat information. STIX is structured so that users can describe threat:

- Motivations
- Abilities
- Capabilities
- Response

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection, and response, etc.

2.2 Cyber Security Information Sharing Framework Elements

Technology

2.2.4 Mechanism of Information Exchange

TAXII's goal is to help add automation to the processes of existing cyber threat cybersecurity information sharing communities and to help establish new communities of sharing by simplifying the technical aspects of cyber threat information exchange. Sharing models supported by TAXII include (but are not limited to):

Source – Subscriber

A single source gathers information and disseminates it out to a community. This is often in the form of a threat monitoring and vulnerability service. This is also a common model for free alerts from some authoritative source.

Hub and Spoke

The hub and spoke model is where a single entity collects information from several other entities. If a piece of information must be shared, it passes through the hub, and then to other entities, or spokes.

Peer to Peer

Information is shared directly with a single other entity. This information is often encrypted, so other parties cannot intercept it.

SECTION 3

ROLES AND RESPONSIBILITIES OF STAKEHOLDERS

This National Cybersecurity Information Sharing Framework is intended to inform, apply, and guide the activities of the key stakeholders across the UAE cyberspace including government ministries, individual entities, industry sectors, and national level organizations. These key stakeholders drive the implementation of the processes, procedures, and capabilities of national cybersecurity information sharing.

Government ministries, authorities, and institutions that operate critical systems, including systems that support the needs of individual government agencies and decision makers that are deemed “very Important” are required to share their information as described below:

Cyber Security Council (CSC)

As the authority for defending and securing the UAE's cyberspace, CSC plays the lead role in developing, promoting, and institutionalizing the environment, working to cultivate and maintain a culture of trust that promotes a need to share responsibly. CSC encourages participation by all relevant stakeholders and plays an active part in integrating existing capabilities to prevent duplicative efforts and increase efficiencies. In this role, CSC will:

1. Serve as the lead entity for the National Cybersecurity Information Sharing Ecosystem (ISE);
2. Gather various types of information from multiple sources.
3. Fuse and analyze that information, transforming it into easily understood formats (i.e., sanitized strategic and tactical analysis that is disseminated to sector regulators, CII operators, and government organizations) via appropriate dissemination channels.
4. Provide the required resources as appropriate to develop cybersecurity information sharing mechanisms, processes, and technology to safeguard information from unauthorized disclosure and use.
5. Promote partnerships and other activities with nations and international organizations as appropriate to facilitate the sharing of information based on common interests, including defining classified and sensitive diplomatic information to be shared and the medium & due care measures of such sharing.
6. Share open information with international partners that support increasing technological knowledge, and facilitate the development of common procedures, processes, and capabilities for cyber security.
7. Manage access to the cybersecurity information sharing platform. i.e., the system of systems that enables the timely and secure exchange of information across participating stakeholders in the UAE.
8. Invite entities to participate in the cybersecurity information sharing platform, consider nominations from potential entities wishing to participate and approve nominations.
9. Approve connections for CSC-sponsored cybersecurity information sharing systems and networks to participating entities.

3.1 National Level Entities

National level governmental entities such as government ministries, authorities, and institutions that operate critical systems are key participants of the National Cyber ISE and collaborate to promote an understanding of the national cybersecurity threat environment.

1. Share information about incidents, threats, and vulnerabilities to the CSC to provide additional insights into the national threat picture.
2. Share with CSC, strategic analysis, best practices, alerts, and warnings received, countermeasures, and lessons learned.
3. Issue and respond to RFIs to obtain additional information from other public, private, and governmental organizations in the UAE, if required.

3.1 National Level Entities

Emirates Lead Entities

Emirates level lead entities are key participants of the National Cyber ISE and collaborate to promote an understanding of the national cybersecurity threat environment.

1. Share information with CSC on the state of cyber security across the emirate (based on specific reporting by government entities) to facilitates situational awareness and coordinated response in the UAE.
2. Share information obtained (e.g., strategic risks) and/or emirate specific incident response center (e.g., incident-specific data) with other emirates and CSC to facilitate cross-sector information sharing.
3. The emirate lead entities are listed below.
    - Abu Dhabi Digital Authority
    - Dubai Electronic Security Center
    - Ajman Digital Authority
    - Sharjah e-Government
    - Fujairah e-Government
    - RAK Electronic Government
    - UAQ e-Government

3.1 National Level Entities

Critical Information Infrastructure Sectors

CII sectors are key participants of Sector Specific Cybersecurity information sharing Communities and/or Cross Cybersecurity information sharing Communities. Cybersecurity information sharing among critical infrastructure sectors is essential to counter the dynamic and evolving threat facing CII and enhance resilience. Sectors serve as information brokers acting as intermediaries and providing greater insights at both the national and entity levels.

1. Develop sector specific cybersecurity information sharing plans that are concerned with sector specific exploits or vulnerabilities.
2. Share information with sector regulators (or other designated sector organizations) to facilitate an understanding and assessment of sector-wide risks.
3. Share information with sector regulators on the state of cyber security across the sector (based on entity-specific reporting). In addition, entity reporting of incidents to sector incident response centers to facilitate cyber situational awareness across the sector and coordinated response.
4. Share information obtained by a sector regulator (e.g., strategic risks) and/or sector incident response center (e.g., incident-specific data) with other sectors to facilitate cross-sector cybersecurity information sharing.

3.1 National Level Entities

Other Entities

Any entity (individual or organization) that controls or manages informational resources in the UAE may choose to participate in the cyber security information sharing communities. All these entities have a significant stake in assuring that the UAE remains cybersecure and are invited to participate in the National Cyber ISF. Any entity within the supply chain of CII may consider itself a part of the National Cyber Security ISE.

1. Identify the information needs and information to be shared while adhering to any mandatory reporting requirements.
2. Provide the technology, facilities, and resources necessary to protect and safeguard information that is obtained through the CSC-sponsored cyber security information sharing platform.

General Populace

It is important for UAE’s general populace to understand their role in securing their personal and professional cyberspace, practice cyber hygiene at all times to support building a safer and more resilient cyber ecosystem. Therefor responsibilities of general populace include:

1. Be recipients of cyber threat information being shared by National level entities.
2. Being aware of cybersecurity information published on social media platforms and websites of National level entities
3. Report any threats/vulnerabilities or risks identified.

SECTION 4

MONITORING AND PERFORMANCE MANAGEMENT

The national cybersecurity ISF outlines measures for monitoring and evaluating progress towards the following objectives:

- Promote transparency and effective management of the national cybersecurity ISF;
- Measure the success of the ISF in a timely manner through performance-based metrics; and
- Provide guidance for improvement and taking necessary intervention steps when appropriate.

To enhance capabilities to share cybersecurity ISF, CSC will work with participating stakeholders in the ISE to obtain feedback on the effectiveness of the framework through cybersecurity information sharing forums, processes, and technology solutions and implementation activities.

Effective cybersecurity information sharing evolves over time because it requires that participants trust and have confidence in the underlying cybersecurity information sharing processes and technology. Tracking the progress of implementation and measuring the effectiveness of the National Cybersecurity ISF is critical to its success. As the National Cybersecurity ISF is implemented, promoted, and institutionalized at the national, sector, and entity levels, the CSC will measure performance and recommend enhancements.

SECTION 5

IMPLEMENTATION

To bring about the change required to successfully promote cybersecurity information sharing, education, awareness, and communications are needed. The CSC will engage participants to promote cybersecurity information sharing as a national and organizational priority. As processes, procedures, and solutions are built to support the collection, analysis, dissemination, and use of information across organizational boundaries, the CSC will educate and raise awareness to provide a foundational understanding and trust among participants. Furthermore, the CSC will work with participating stakeholders to acknowledge stakeholder organizations that contribute information that leads to innovative cyber solutions and connections among disparate sources of information that enhances the resilience of the UAE’s cyberspace.

SECTION 6

APPENDICES

6.1 Acronyms

Usage	Description
AES	Advanced Encryption Standard
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIA	Confidentiality, Integrity and Availability
DES	Data Encryption Standard
FDE	Full Disk Encryption
FLE	File Level encryption
ICT	Information and Communications Technology
IoC	Indicators of Compromise
IP	Internet Protocol
ISE	Information Sharing Environment
ISAC	Information Sharing and Analysis Centers
ISC	Information Sharing Community
ISE	Information Sharing Environment
ISF	Information Sharing Framework
NCIS	National Cyber Information Sharing
SHA	Secure Hash Algorithm
TTP	Tactics, Techniques, and Procedures

6.2 Structured Threat Information Expression Structure (STIX)

The cybersecurity information sharing processes must be flexible, to provide a variety of methods of communication. It is necessary to respond to the predicted needs of the participating entities and possible situations to be able to collect threat information.

The method that the UAE will be using to identify, share, and analyze will be based on the Structured Threat Information Expression structure. Otherwise known as STIX, this informational structure is based on 9 key constructs:

Construct	Information Collected	Information Shared
Observables	The properties or events pertinent to the operation of computer networks will be collected. File names, Registry values, IP watchlists, fields, and access logs will be collected. Property patterns will also be collected.	Information shared must include single objects, object patterns, or multiple objects, are that indicate potential threats, threat campaigns, or threat adversaries.
Indicators	One or more specific observable patterns that represent artifacts and behaviors of interest. They are combined with contextual metadata that indicate likely impact or confidence amongst other necessary information.	Observed patterns in a Cybersecurity context that indicate behaviors of interest the Information Sharing Community will benefit from understanding.

6.2 Structured Threat Information Expression Structure (STIX)

Construct	Information Collected	Information Shared
Incidents	The indicator patterns, time bound into response investigations. These incidents will include parties involved, confidence levels, and action logs amongst others.	Incident patterns that will improve the Information Sharing Communities security and threat environment understanding.
Adversary Tactics, Techniques, and Procedures (TTP)	The modus operandi of cyber threats. This includes the techniques and tactics of specific adversaries, such as identifying individuals and malware.	When the entity has connected gathered information to a specific adversary, this will be shared with the Information Sharing Community.
Exploit Targets	The vulnerabilities in entity software or personnel that will be targeted for exploitation. Day one weaknesses, common vulnerabilities, and handling guidance will be collected.	Common Configuration Enumeration, Common Weakness Enumeration, and the Common Vulnerability Reporting Framework will be consulted when sharing information.
Courses of Action	The measures taken to address threats, successful or not, corrective or preventative.	The impact of, cost of, efficacy of, and guidance of will be shared to improve the ISC's security.

6.2 Structured Threat Information Expression Structure (STIX)

Construct	Information Collected	Information Shared
Campaigns	Sets of incidents that indicate a threat actor is pursuing a goal. This will include sets of related incidents, composed of related patterns.	The incidents sets, and the context that indicates they are related, along with successful mitigation measures.
Threat Actors	The characterizations of malicious actors constructed by observed behaviors. Suspected motivation, effects, TTP, and relationships with other threat actors.	Handling guidance, confidence level, source of information, along with the necessary context and metadata to improve the Information Sharing Communities Threat Actor structure.
Reports	Automated Vulnerability Report Documentation will be created according to the Trusted Automated eXchange of Intelligence Information. (TAXII). This information can enable multiple methods of information sharing, from peer to peer to hub and spoke.	Reports collect the context in which the other constructs have been observed and share the reason(s) why these constructs must be shared.

Thus, any cybersecurity information sharing community operating in the UAE should follow both STIX and TAXII documentation of cyber incidents. They must separate the threat information collected and the threat information to be shared, the conditions under which it will be shared, and identify approved recipients of their threat information according to the traffic light protocol.

They must also review the TAXII, STIX and Traffic Light Protocol to rate the information appropriately, along with sanitizing the threat information and metadata well.

6.3 Traffic Light Protocol (TLP)

The Traffic Light Protocol, from RED to WHITE, is a globally used best practice method of identifying sharing designations. These designations identify threat information that may be suitable for release and/or information that is not suitable for release. Each UAE ISC will develop their own designations that will assist in the sharing of information.

The Traffic Light Protocol specifies restrictions that apply to Threat Information. As with the rest of the shared information, sharing entities may decide on their own how they wish to share their information. They may choose to share the collection processes or technology used or they may not, depending on the TLP level they have chosen.

The entities must decide the types of report they are willing to share at each level, and how they will designate the share ability of said information before they write and disseminate their reports.

Color	When should it be used?	How may it be shared?
TLP:RED 🔴 ⚪ ⚪ Nor for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impact on a party’s privacy, reputation, or operations if misused	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meetings, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally in person.
TLP:AMBER ⚪ 🟡 ⚪ Limited disclosure, restricted to participant's’ organizations	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may not share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.**

6.3 Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
TLP:GREEN ○ ○ 🟢 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may not share TLP:GREEN information with peers and partners organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ○ ○ ○ Disclosure not limited	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.