**1654: Cyber Incident Reporting**

**When to Report**

A federally insured credit union that experiences a reportable cyber incident must report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident.

***Reportable cyber incident***
A reportable cyber incident is any substantial cyber incident that leads to one or more of the following:

1. A substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes.
2. A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.
3. A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

A *reportable cyber incident* does not include any event where the cyber incident is performed in good faith by an entity in response to a specific request by the owner or operators of the system.

***Definitions***

* **Compromise:**the unauthorized disclosure, modification, substitution, or use of sensitive data or the unauthorized modification of a security-related system, device, or process in order to gain unauthorized access.
* **Confidentiality:** preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
* **Cyber incident:** an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.
* **Cyberattack:** an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
* **Disruption:** an unplanned event that causes an information system to be inoperable for a length of time.
* **Integrity:** guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
* **Sensitive data:** any information which by itself, or in combination with other information, could be used to cause harm to a credit union or credit union member and any information concerning a person or their account which is not public information, including any non-public personally identifiable information.

**How to Report**
To report a cyber incident, federally insured credit unions may notify the NCUA through the following channels:

* NEW [NCUA Online Cyber Incident Reporting System](https://cyberreports.ncua.gov/dcs_external?id=dcs_ext_cat_item&sys_id=8ac330ad47174e50c6cdf9ee626d43cb" \t "_blank)
* Call the NCUA at 1-833-CYBERCU (1-833-292-3728) and leave a voicemail; or,
* Use the [National Credit Union Administration Secure Email Message Center](https://web1.zixmail.net/s/login?b=ncua) to send a secure email to cybercu@ncua.gov.

**What to Report**
Federally insured credit unions should be prepared to provide the following information, if known, at the time of reporting.

* Reporter Name and Title: Name and title of individual reporting the incident
* Callback Number: Best callback number for the NCUA to contact regarding the incident
* Charter Number: Do not include leading zeros
* Credit Union Name: Name of affected credit union
* Date and Time Identified: The date and time the credit union reasonably believes a reportable cyber incident took place
* Description: A general description of the reportable cyber incident:
	+ What services were impacted?
	+ Was sensitive data or member information compromised?
	+ What impact did it have on operations?

At the time of initial notification, do not send the NCUA

* Sensitive personally identifiable information;
* Indicators of compromise;
* Specific vulnerabilities; or
* Email attachments.