

Note: The following appendix will not appear in the Code of Federal Regulations.

Form SCIR

Significant Cybersecurity Incidents and Risks

OMB Approval	
OMB Number:	<input type="checkbox"/>
Expires:	<input type="checkbox"/>
Estimated average burden hours per response:	<input type="checkbox"/>
per amendment:	<input type="checkbox"/>

FORM SCIR INSTRUCTIONS

A. GENERAL INSTRUCTIONS

1. **FORM** – Part I of Form SCIR must be used by a covered entity to confidentially report a cybersecurity incident pursuant to the requirements of 17 CFR 242.10. Part II of Form SCIR must be used to publicly disclose cybersecurity risks and significant cybersecurity incidents pursuant to the requirements of 17 CFR 242.10.
2. **ELECTRONIC FILING** - A covered entity must file Parts I and II of Form SCIR through the EDGAR system, and must utilize the EDGAR Filer Manual (as defined in 17 CFR 232.11) to file Parts I and II of Form SCIR electronically to assure the timely acceptance and processing of the filing. Refer to 17 CFR 242.10 for other requirements with respect to filing Part I of Form SCIR with other regulators and for other requirements with respect to publicly disclosing Part II of Form SCIR.
3. **FEDERAL INFORMATION LAW AND REQUIREMENTS** - An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. Sections 15F, 17(a), 17A, and 23(a) of the Exchange Act authorize the U.S. Securities and Exchange Commission (“Commission”) to collect the information on Form SCIR from covered entities. See 15 U.S.C. §§78o-10, 78q and 78w. Filing of Parts I and II Form SCIR is mandatory. The principal purpose of Part I of Form SCIR is to report information about a significant cybersecurity incident impacting a covered entity so the Commission can respond to the incident, evaluate the operating status of the covered entity, and assess the impact the significant cybersecurity incident may have on other participants in the U.S. securities markets. The principal purpose of Part II of Form SCIR is to publicly disclose summary descriptions of the cybersecurity risks of the covered entity and summary descriptions of each significant cybersecurity incident that covered entity has experienced in the current or previous calendar year (if applicable). Any member of the public may direct to the Commission any comments concerning the accuracy of the burden estimate on this form, and any suggestions for reducing this burden. This collection of information has been reviewed by the Office of Management and Budget in accordance with the clearance requirements of 44 U.S.C. §3507. The information contained in this form is part of a system of records subject to the Privacy Act of 1974, as amended. The Commission has published in the Federal Register the Privacy Act Systems of Records Notice for these records.
4. **FORMAT**
 - a. All Items must be answered and all fields requiring a response must be completed before the filing will be accepted.
 - b. A covered entity must complete the execution screen certifying that Form SCIR has been executed properly and that the information contained in the form is accurate and complete before the filing will be accepted.
 - c. A paper copy, with original signatures, of Part I and Part II of Form SCIR must be retained by the covered entity and be made available for inspection upon a regulatory request.
5. **EXPLANATION OF TERMS**
 - a. **COVERED ENTITY** – The term “covered entity” has the same meaning as that term is defined in 17 CFR 242.10 and, as used in Form SCIR, also refers to the person filing the Form.
 - b. **CYBERSECURITY INCIDENT** – The term “cybersecurity incident” has the same meaning as that term is defined in 17 CFR 242.10.
 - c. **CYBERSECURITY RISK** – The term “cybersecurity risk” has the same meaning as that term is defined in 17 CFR 242.10.
 - d. **INTERNAL INVESTIGATION** – The term “internal investigation” means a formal investigation of the significant cybersecurity incident by internal personnel of the covered entity or external personnel hired by the covered entity that seeks to determine any of the following: the cause

of the significant cybersecurity incident; whether there was a failure to adhere to the covered entity's policies and procedures to address cybersecurity risk; or whether the covered entity's policies and procedures to address cybersecurity risk are effective.

- e. **PERSONAL INFORMATION** – The term “personal information” has the same meaning as that term is defined in 17 CFR 242.10].
- f. **SIGNIFICANT CYBERSECURITY INCIDENT** – The term “significant cybersecurity incident” has the same meaning as that term is defined in 17 CFR 242.10.
- g. **UNIQUE IDENTIFICATION CODE** – The term “unique identification code” means a unique identification code assigned to a person by an internationally recognized standards-setting system that is recognized by the Commission pursuant to Rule 903(a) of Regulation SBSR (17 CFR 242.903(a)).

B. INSTRUCTIONS TO PART I OF FORM SCIR

1. **INITIAL REPORT** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must file an initial report on Part I of Form SCIR with respect to a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.
2. **AMENDED REPORT** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must file an amended report on Part I of Form SCIR with respect to a significant cybersecurity incident after each of the following circumstances:
 - Any information on a previously filed Part I of Form SCIR pertaining to the significant cybersecurity incident becomes materially inaccurate;
 - Any new material information pertaining to a significant cybersecurity incident previously reported to the Commission on Part I of Form SCIR being discovered;
 - A significant cybersecurity incident is resolved; or
 - An internal investigation pertaining to a significant cybersecurity incident is closed.
3. **FINAL REPORT** - A covered entity filing a final report on Part I of Form SCIR must indicate on the final notification if: (i) the Part I of Form SCIR is being filed because the significant cybersecurity incident has been resolved and either no internal investigation pertaining the significant cybersecurity incident is being or will be conducted or an internal investigation pertaining to the significant cybersecurity incident has been closed prior to the resolution of the incident; or (ii) the Part I of Form SCIR is being filed to report that an internal investigation pertaining to the significant cybersecurity incident has been closed and the significant cybersecurity incident is resolved. If a covered entity files a final report on Part I of Form SCIR with respect to a significant cybersecurity incident, and, thereafter, conducts an internal investigation pertaining to the significant cybersecurity incident, it must file another final report on Part I of Form SCIR when the investigation is closed pursuant to the requirements of 17 CFR 242.10.
4. **CONTACT EMPLOYEE** - The individual listed as the contact employee must be authorized by the covered entity to provide the Commission with information about the significant cybersecurity incident, and make information about the significant cybersecurity incident available to the Commission.
5. **LINE ITEMS**
 - a. **Line 2** – Provide the date the covered entity had a reasonable basis to conclude that the significant cybersecurity incident had occurred or was occurring. This can be based on, for example, reviewing or receiving a record, alert, log, or notice about the incident.
 - b. **Line 3.C.** – Provide the approximate date that the Covered Entity was no longer undergoing a significant cybersecurity incident.

C. INSTRUCTIONS TO PART II OF FORM SCIR

- 1. PUBLIC DISSEMINATION** – Part II of Form SCIR will be publicly disseminated upon filing it with the Commission.
- 2. DISCLOSURE UPDATES** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must promptly provide an updated disclosure through the methods required by 17 CFR 242.10 if the information required to be disclosed pursuant to 17 CFR 242.10 materially changes, including after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

The mailing address for questions and correspondence is:

**The Securities and Exchange Commission
Washington, DC 20549**

FORM SCIR PART I		SIGNIFICANT CYBERSECURITY INCIDENTS		Official Use
Page 1 (Execution Page)		Date: _____ SEC Filer No: _____		Official Use Only
WARNING	Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action.			
	INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS. See 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)			
INITIAL REPORT <input type="checkbox"/>		AMENDED REPORT <input type="checkbox"/>		FINAL AMENDED REPORT <input type="checkbox"/>
				Check the reason for filing the Final Amended Report
				Incident Resolved <input type="checkbox"/>
				Investigation Closed <input type="checkbox"/>
1. Information about the <i>covered entity</i> :				
A. i. Full legal name: _____				
ii. Business name if different than legal name: _____				
B. Tax Identification No.: _____		Covered Entity's UIC # (if any): _____		Covered Entity's CIK #: _____
C. Main Address: (Do not use a P.O. Box)				
Number and Street 1: _____		Number and Street 2: _____		
City: _____	State: _____	Country: _____	Zip/Postal Code: _____	
D. Contact Employee				
Name: _____		Phone Number: _____		Email: _____
E. Type of <i>Covered Entity</i> (Check all that apply):				
Broker or dealer <input type="checkbox"/>		Clearing Agency <input type="checkbox"/>		Major Security-Based Swap Participant <input type="checkbox"/>
Municipal Securities Rulemaking Board <input type="checkbox"/>		National Securities Association <input type="checkbox"/>		National Securities Exchange <input type="checkbox"/>
Security-Based Swap Dealer <input type="checkbox"/>		Security-Based Swap Data Repository <input type="checkbox"/>		Transfer Agent <input type="checkbox"/>
EXECUTION:				
The undersigned certifies that this form was executed on behalf of, and with the authority of, the covered entity. The undersigned and covered entity represent that the information and statements contained herein are current, true and complete. The undersigned and covered entity further represent that to the extent any information previously submitted is not amended such information is current, true, and complete.				
_____ Date (MM/DD/YYYY)		_____ Full Legal Name of Covered Entity		
By: _____ Signature		_____ Name and Title of Person Signing on Covered Entity's behalf		
<i>This page must always be completed in full.</i>				
DO NOT WRITE BELOW THIS LINE – FOR OFFICIAL USE ONLY				

FORM SCIR PART I Page 2	Covered Entity Name: _____	Official Use	<small>Official Use Only</small>		
	Date: _____ SEC Filer No: _____				
2. The approximate date the significant cybersecurity incident was discovered:		<input type="text"/> DD	<input type="text"/> MM	<input type="text"/> YYYY	
3. The approximate duration of the significant cybersecurity incident:					
A. Is the incident ongoing: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/>					
B. Approximate start date of incident:					
		<input type="text"/> DD	<input type="text"/> MM	<input type="text"/> YYYY	Unknown <input type="checkbox"/>
C. Approximate date incident was resolved:					
		<input type="text"/> DD	<input type="text"/> MM	<input type="text"/> YYYY	
4. The status of an internal investigation pertaining to the significant cybersecurity incident:					
A. Is an internal investigation being conducted: Yes <input type="checkbox"/> No <input type="checkbox"/>					
B. If are yes, approximate date the internal investigation was closed:					
		<input type="text"/> DD	<input type="text"/> MM	<input type="text"/> YYYY	
5. Has a law enforcement or government agency (other than the Commission) been notified of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/>					
If yes, identify each law enforcement or government agency: _____					

6. Describe the nature and scope of the significant cybersecurity incident, including the information systems affected by the incident and any effect on the covered entity's critical operations:					

7. A. Has the threat actor(s) causing the significant cybersecurity incident been identified: Yes <input type="checkbox"/> No <input type="checkbox"/>					
If yes, identify the threat actor(s): _____					

B. Has there been communication(s) from or with the threat actor that caused or claims to have caused the significant cyber security incident (answer even if the actor(s) has not been identified): Yes <input type="checkbox"/> No <input type="checkbox"/>					
If yes, describe the communications: _____					

FORM SCIR PART I Page 3	Covered Entity Name: _____	Official Use	Official Use Only
	Date: _____ SEC Filer No: _____		
8. Describe the actions taken or planned to respond to and recover from the significant cybersecurity incident: _____ _____ _____ _____			
9. Was any data stolen, altered, or accessed or used for any other unauthorized purpose: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the nature and scope of the data: _____ _____ _____			
10. A. Was any personal information lost, stolen, modified, deleted, destroyed, or accessed without authorization as a result of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the nature and scope of the information: _____ _____ _____ B. i. If yes, has notification been provided to persons whose personal information was lost, stolen, modified, deleted, destroyed, or accessed without authorization: Yes <input type="checkbox"/> No <input type="checkbox"/> ii. If no, is notification planned: Yes <input type="checkbox"/> No <input type="checkbox"/>			

FORM SCIR PART I Page 4	Covered Entity Name: _____	Official Use	Official Use Only						
	Date: _____ SEC Filer No: _____								
11. Were any assets of the covered entity lost or stolen as a result of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known: _____ _____ _____ _____ _____									
12. A. Were any assets of the covered entity's customers, counterparties, members, registrants, or users lost or stolen as a result of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known: _____ _____ _____ _____									
B. i. If yes, has notification been provided to persons whose assets were lost or stolen: Yes <input type="checkbox"/> No <input type="checkbox"/> ii. If no, is notification planned: Yes <input type="checkbox"/> No <input type="checkbox"/>									
13. Has the significant cybersecurity incident been disclosed in accordance with 17 CFR 242.10: A. On EDGAR: Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, disclosure date: <table border="1" style="display: inline-table;"><tr><td>DD</td><td>MM</td><td>YYYY</td></tr></table> B. On business Internet website: Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, disclosure date: <table border="1" style="display: inline-table;"><tr><td>DD</td><td>MM</td><td>YYYY</td></tr></table> C. If applicable, to the covered entity's customers: Yes <input type="checkbox"/> No <input type="checkbox"/> If 12.A, 12.B, and/or 12C. are no, explain why the disclosures have not been made: _____ _____ _____ _____				DD	MM	YYYY	DD	MM	YYYY
DD	MM	YYYY							
DD	MM	YYYY							
14. A. Is the significant cybersecurity incident covered by an insurance policy of the covered entity: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> B. If yes, has the insurance company been contacted: Yes <input type="checkbox"/> No <input type="checkbox"/>									
15. Provide any additional information or comments: _____ _____ _____ _____									

FORM SCIR PART II Page 1 (Execution Page)	CYBERSECURITY RISKS AND SIGNIFICANT CYBERSECURITY INCIDENTS Date: _____ SEC File No: _____	Official Use	Official Use Only
WARNING	Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action. INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS. See 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)		
1. Information about the covered entity:			
A. i. Full legal name: <input type="text"/> ii. Business name if different than legal name: <input type="text"/>			
B. Covered Entity's UIC # (if any): <input type="text"/> Covered Entity's CIK #: <input type="text"/>			
C. Main Address: (Do not use a P.O. Box) Number and Street 1: <input type="text"/> Number and Street 2: <input type="text"/> City: <input type="text"/> State: <input type="text"/> Country: <input type="text"/> Zip/Postal Code: <input type="text"/>			
D. Type of Covered Entity (Check all that apply): Broker or dealer <input type="checkbox"/> Clearing Agency <input type="checkbox"/> Major Security-Based Swap Participant <input type="checkbox"/> Municipal Securities Rulemaking Board <input type="checkbox"/> National Securities Association <input type="checkbox"/> National Securities Exchange <input type="checkbox"/> Security-Based Swap Dealer <input type="checkbox"/> Security-Based Swap Data Repository <input type="checkbox"/> Transfer Agent <input type="checkbox"/>			
EXECUTION: The undersigned certifies that this form was executed on behalf of, and with the authority of, the covered entity. The undersigned and covered entity represent that the information and statements contained herein are current, true and complete. The undersigned and covered entity further represent that to the extent any information previously submitted is not amended such information is current, true, and complete.			
<input type="text"/> Date (MM/DD/YYYY) By: <input type="text"/> Signature		<input type="text"/> Full Legal Name of Covered Entity <input type="text"/> Name and Title of Person Signing on Covered Entity's behalf	
<i>This page must always be completed in full.</i>			
DO NOT WRITE BELOW THIS LINE – FOR OFFICIAL USE ONLY			

FORM SCIR PART II Page 2	Covered Entity Name: _____	Official Use	Official Use Only
	Date: _____ SEC File No: _____		
<p>2. "Cybersecurity risk" means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities. "Cybersecurity incident" means an unauthorized occurrence on or conducted through a covered entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems. "Cybersecurity threat" means any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a covered entity's information systems or any information residing on those systems. "Cybersecurity vulnerability" means a vulnerability in a covered entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.</p> <p>Provide a summary description of the cybersecurity risks that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks.</p> <hr/> <hr/> <hr/> <hr/>			
<p>3. A "significant cybersecurity incident" means a cybersecurity incident, or a group of related cybersecurity incidents, that:</p> <p>(1) significantly disrupts or degrades the ability of the covered entity to maintain critical operations; or</p> <p>(2) leads to the unauthorized access or use of the information or information systems of the covered entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in:</p> <p>(A) substantial harm to the covered entity; or (B) substantial harm to a customer, counterparty, member, registrant, or user of the covered entity, or to any other person that interacts with the covered entity.</p> <p>Has the covered entity experienced one or more significant cybersecurity incidents during the current or previous calendar year: Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>If yes, provide a summary description of each significant cybersecurity incident during that period. The description of <u>each</u> significant cybersecurity must include, at a minimum, the following information to the extent known:</p> <p>The person or persons affected;</p> <p>The date the incident was discovered and whether it is ongoing;</p> <p>Whether any data was stolen, altered, or accessed or used for any other authorized purpose;</p> <p>The effect of the incident on the covered entity's operations; and</p> <p>Whether the covered entity, or service provider, has remediated or is currently remediating the incident.</p> <hr/> <hr/> <hr/> <hr/> <hr/>			