1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	CISA Incident Reporting Form
15	Complete Question Set
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	

Table of Contents

31	Table of Contents	2
32	a. Introduction	5
33	b. Labels Used	5
34	c. Beginning of Incident Reporting Questions	6
35	d. Report Type	6
36	e. Report Reason	7
37	f. Contact Information of Reporter:	9
38	g. Impacted Entity Demographics	11
39	h. Incident Overview	25
40	Incident Category Type Determination	25
41	i. Incident Notifications	27
42	j. Incident: Severity Assessments	
43	Confidentiality, Integrity, Availability (CIA) Assessment	
44	Violation of Law and Policy	
45	Incident: High-Level Impacts	
46	Public Impacts	
47	National US Impacts	
48	Regional Impacts (Local to Global)	
49	Breach Severity Impacts	
50	Major Incident Severity Determination (FISMA Only)	
51	Public Health and Safety Impacts	
52	Indirect Impacts	
53	Impacts Internal to the Entity	
54	Functional Impacts to Entity	
55	Informational Impacts to Entity	
56	Physical Impacts to Entity	
57	Economic Impacts to Entity	
58	k. Incident Details	
59	Incident: Details by Stage	
60	1. Identification and Detection (I/D) Stage	
61	Incident Stage (I/D): Ransomware and Cyber Extortion	

62	Initial Ransom Demand Details	41
63	Ransom Payment Details	42
64	Results of Ransom Incident	46
65 66	Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) and Indicators of Compromise (I Observed	OCs) 47
67	Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) Observed	48
68	Incident Stage (I/D): Indicators of Compromise (IOCs) and associated Detection Methods Used	50
69	Indicator of Compromise (IOC) Individual Data Marking	55
70	Incident Stage (I/D): Indicators of Compromise (IOCs): Detection Methods	55
71	Incident Stage (I/D): Malware Artifacts and Detection Logics/Analytics	57
72 73	Incident Stage (I/D): Malware Artifacts and Detection Logics/Analytics: Data Classification Markings	58
74	Incident Stage (I/D): Data Sources Used and Attribution	58
75	Data Sources Used	58
76	Attribution	58
77	m. Assistance	59
78	Assistance from CISA	59
79	Third Party Assistance	59
80	Data Sharing and Logging Readiness	59
81	n. Analysis (A) Stage	61
82	Incident Stage (A): Impacted Users and Systems	62
83	Incident Stage (A): Initial Access "Patient Zero" Details	67
84	Incident Stage (A): Detailed Informational Impacts	68
85	Incident Stage (A): Breach Details	73
86	Impacted Individuals	74
87	PII Accessed and/or Impacted	74
88	Incident Stage (A): Security Control(s) [Contributing to Incident]	78
89	o. Containment (C) Stage	80
90	Incident Stage (C): Countermeasures – Containment	81
91	p. Eradication Stage	83
92	Incident Stage (E): Countermeasures – Eradication	84
93	q. Recovery (R) Stage	85
94	Incident Stage (R): Recovery Actions	86
95	r. Post-Incident (P-I) Stage	87

96	s. Event Reporting (Below Incident Thresholds) (FISMA – Only)	89
97	t. Data Marking Stage	90
98	Cybersecurity Information Sharing Act of 2015 Acknowledgement	90
99	Overall Report Data Markings	90
100	u. End of Incident Reporting Questions	90
101	v. Appendix 1: Data Marking	90
102	Data Marking Options	90
103	w. Appendix 2: CISA Cybersecurity Performance Goals (Protect) & NIST SP 800-53 References	91
104	Protect CISA CPGs & NIST SP 800-53 References	91
105	x. Appendix 3: Incident Type/Categories	99
106	Incident Types involving Malware	99
107	Incident Types Involving Hacking	. 100
108	Incident Types Involving Social Engineering	. 101
109	Incident Types Involving Misuse of Assets	. 101
110	Incident Types Involving Physical Actions	. 102
111	Incident Types Involving Human (or Technology) Errors	. 102
112	Incident Types Involving Environmental Factors	. 103
113	y. Appendix 4: Critical Infrastructure Sectors and Subsectors	. 103
114	z. Appendix 5: Federal Agencies and Sub-Agencies	. 107
115		
116		
117		
118		
119		
120		
121		
122		
102		
123		
124		
125		
126		
127		

128 **a. Introduction**

- 129 The Cybersecurity and Infrastructure Security Agency (CISA) collects cybersecurity incident
- 130 reports related to federal agency information systems, mandatory reports on behalf of certain
- 131 federal regulatory agencies, mandatory reports due to contractual requirements, and voluntary
- reports from members of the public. This question set, which is authorized by the Federal
- 133 Information Security Modernization Act of 2014 (FISMA) and the Homeland Security Act, is
- distinct from incident reporting under the Cyber Incident Reporting for Critical Infrastructure
 Act (CIRCIA). CISA will use a different information collection instrument for CIRCIA incident
- 136 reports after the effective date of CIRCIA implementing regulations.
- 137 The questions included in this document represent the universe of all possible questions CISA
- 138 may use for incident report information collection purposes across the multiple existing incident
- 139 reporting use cases; no respondent will be presented all the questions. In the Incident Reporting
- 140 Portal respondents will be directed to answer a subset of the questions based on the characteristics
- 141 of the reporting entity, the reasons for which they are reporting, and the nature of the incident. The
- 142 dynamic design of the Incident Reporting Portal means that the user experience flow from question
- to question is driven by the individual respondent's responses. As described in the next section
- 144 CISA has provided design notes to explain the conditional logic which supports the dynamic design;
- the conditional logic may change as CISA works to implement the Incident Reporting Portal and is
- 146 provided as an example to help the reader understand how questions relate to one another.

147 **b.Labels Used**

- 148 Throughout this document labels are used to provide context on how conditional logic may 149 impact the flow from question-to-question, to indicate where certain respondents may be able to 150 indicate they would like certain data markings applied to their responses to the question, and to
- note where additional text may be shown to the respondent in the Incident Reporting Portal to
- 152 assist with question comprehension.
- 153 Conditional Logic Markings:

154	[RA] = Required question for all types of reports
155 156 157	[RR] = Required question for reports identified as necessary to satisfy a regulatory and/or statutory requirement including Federal Information Security Modernization Act (FISMA)
158	[RC] = Required question based on an earlier conditional response/selection.
159 160	[FISMA Req] = Required question for reports identified as necessary to satisfy FISMA reporting requirements.
161 162	[FedRAMP] = Required question for reports identified as necessary to satisfy Federal Risk and Authorization Management Program (FedRAMP) reporting requirements.
163	[Fed Ctr] = U. S. Government Federal Contractor Only

164	[Op] = Optional
165 166	[Op] + [FISMA Req] = Required for FISMA reporters and optional for all other reporters.
167 168	[Op] + [RR] = Optional for all, except required for regulatory and/or statutory reporting including FISMA.
169	{Conditional} = Provides additional conditional logic context on some questions.
170	Data Markings:
171 172 173	[C-15] = CISA 2015 data marking option for <u>non-Federal incident reporting</u> . This is not a default marking but is available for non-Federal reporters if their data meets CISA 2015 data marking criteria, e.g., cyber threat indicators (CTIs).
174	[CUI] = Controlled unclassified information
175	Design and display note markings:
176	Display notes do not contain questions with which a respondent must engage. Display
177 178	notes contain additional explanatory content which may assist a respondent with responding to a question. The format for these notes is as follows:
170	responding to a question. The format for these notes is as follows.
179	(DISPLAY NOTE: Light blue and bolded words should be displayed to the reader.)
180 181 182	All Footnotes contained in this document accompany Display Notes and will be presented on the form in a method determined during the design process for the best display for the reader. These methods could be a combination of "pop-ups", on form notes, "hover-over" notes, etc.
183	Design notes are intended to enable the developers of the Incident Reporting Portal and
184	reviewers of the question understand the conditional logic which may direct a respondent
185	from one question to the appropriate next question based on their input. The flow from
186	question-to-question will continue to be under development as CISA incorporates
187	feedback from reviewers. However, since it is critical to communicate that no respondent
188	will answer all the questions contained herein, we wanted to provide this conditional
189 190	logic to support reviewers' understanding of how the dynamic form may work. The format for these notes is as follows:
190	format for these notes is as follows.
191 192	(DESIGN NOTE: Black and bolded words are for the developers only and should not be displayed to the readers.)

193 c. Beginning of Incident Reporting Questions

194

(DISPLAY NOTE: Global Disclaimer: Please fill out all questions in this form to the best of your knowledge at the time of
 submission.)

197 **d. Report Type**

199	FOR ALL REPORTERS
200	1. [RA] What type of report do you want to submit?
201	A. Initial report
202	B. Supplemental/update report
203	C. Post-incident report ¹
204	e. Report Reason
205	2. [RA] Why are you reporting? (DESIGN NOTE: Single select)
206	A. Voluntarily reporting a cyber incident (select one) (DESIGN NOTE: If voluntary is
207	selected, display the two following types of voluntary reporting and single select)
208	1. Are you voluntarily reporting an incident for an individual (yourself or
209	another person)?
210	2. Are you voluntarily reporting an incident for an entity (a company,
211	organization ² , etc.)?
212	B. Reporting to satisfy a regulatory, statutory, and/or contractual requirement
213	(DISPLAY NOTE: If you are a third party completing the incident report on behalf of the affected entity,
214 215	please be aware that we ask for details about the affected organization first and will gather your details later in the process)
216	3. {Conditional on selecting "2.B" above}[RR] Please identify the regulatory, statutory,
217	and/or contractual requirement you are intending to satisfy with this report from the
218	list below. (DESIGN NOTE: Multi select) (DESIGN NOTE: This question does not apply to "voluntary"
219	identified reports)
220	(DISPLAY NOTE: To the extent that a reporting requirement provides that reporting to CISA is a means
221	of compliance, you must indicate the specific requirement below to be considered as reporting under that requirement)
222	A Cybersecurity and Infrastructure Security Agency (CISA)
224	1. Federal Information Security Modernization Act of 2014 (FISMA 2014)
225	a. Please select the appropriate report reason:
226	1. Cyber incident
227	2. Unauthorized release and/or loss of agency information
228	(including personally identifiable information) unrelated to a
229	cybersecurity incident
220	eysenseemity merdent
230	B Federal Energy Regulatory Commission (FERC)/ North American Electric
201	D. Federal Energy Regulatory Commission (FERC)/ North American Electric Daliability Corporation (NEDC)
232	Kenadinty Corporation (NEKC)

¹ **Post Incident "Stage" [Report]:** Report submitted at the conclusion of the incident after all recovery efforts have been completed (or at a minimum, completed efforts have been accepted by the impacted entity as sufficient). The post incident report includes information referenced in CISA's Incident Response Playbook, such as documenting lessons learned. For Federal Civilian Executive Branch reporters, this post incident report is due no later than 7 days after incident resolution.

² Organization: [FIPS 200, https://doi.org/10.6028/NIST.FIPS.200] An entity of any size, complexity, or positioning within an organizational structure, including federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or, as appropriate, any of their operational elements.

233	1. Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber
234	Security Management Controls) and CIP-008-6 (Cyber Security – Incident
235	Reporting and Response Planning)
236	
237	C. Federal Risk and Authorization Management Program (FedRAMP)
238	1. Please select the appropriate report reason:
239	a. Cyber incident
240	b. Unauthorized release and/or loss of agency information (including
241	personally identifiable information) unrelated to a cybersecurity
242	incident
243	
244	D. Nuclear Regulatory Commission
245	1. Cybersecurity event notifications (10 C.F.R 73.77)
246	
247	E. Transportation Security Administration (TSA)
248	1. Security Directives or Information Circulars associated with Surface
249	Transportation, Rail, Public Transportation and Passenger Railroad
250	Cybersecurity (SD 1582-21-01 series, SD 1580-21-01 series, and IC 2021-
251	01, including all amendments and successors)
252	2. Security Directives or Information Circulars associated with Pipeline
253	Cybersecurity (SD Pipeline 2021-01 series and IC Pipeline 2022-01,
254	including all amendments and successors)
255	3. (DESIGN NOTE: Placeholder for aviation citations, details TBD)
256	a. Airport Security Program (ASP)
257	b. Aircraft Operator Standard Security Program (AOSSP)
258	c. Full All-Cargo Aircraft Operator Standard Security Program
259	(FACAOSSP)
260	d. Twelve-Five Standard Security Program (TFSSP)
261	e. Private Charter Standard Security Program (PCSSP)
262	f. Indirect Air Carrier Standard Security Program (IACSSP)
263	g. Certified Cargo Screening Standard Security Program (CCSSP)
264	
265	F. U.S. Coast Guard (USCG)
266	1. Suspicious activity, breaches of security, or transportation security incidents
267	(33 C.F.R 101.305 and 33 C.F.R. 6.16)
268	
269	G. Reserved entity for future if necessary {PRA placeholder}
270	1. Reserved statute, regulation, or contractual requirement
271	a. Please select the appropriate report reason:
272	1. (DESIGN NOTE: "report reason" List)

273	
274	H. Other (DISPLAY NOTE: Reporters selecting this option are responsible for confirming that the
275	listed agency and statute/regulation/contract permit reporting to CISA as a means of compliance with
276	that agency's reporting requirements.)
277	1. Agency [describe] (DESIGN NOTE: Open text)
278	2. Statute, regulation, or contract clause [describe] (DESIGN NOTE: Open text)
279	f. Contact Information of Reporter:
280	4. [CUI][RA] Please provide your name and contact information
281	A. [CUI]Name
282	1. First
283	2. Last
284	B. [CUI] Phone number(s)
285	1. Preferred
286	2. Alternate
287	C. [CUI] Email address(es)
288	1 Preferred
289	2 Alternate
205	D [CUII] Social media profile (Optional)
291	1 Primary social media handle or username?
201	 Finter the corresponding social media platform
292	E. Job title
293	E. Which time zone are you in?
294	1. Which the zone are you in:
295	5 [CIIIIR A] Are you the primary point of contact for this incident? (Ves/No)
290	A [CUIIIRC] (DESIGN NOTE: If No) Please provide the primary point of contact name
207	and contact information
290	1 [CIII]Name
300	a First
301	h I ast
302	2 [CIII]Phone number(s)
302	2. [COT] none number(3)
304	h Alternate
305	3 [CIII]Email address(es) of point of contact
306	3. Preferred
207	a. Herente
200	4. [CIII] Social media profile (Optional)
200	[COI] Social media prome (Optional)
309	a. Filinary social media nanule of username?
214	5. Job title
311	5. JOD HHE
312	o. which time zone are they in?

313	
314	6. [RA] Are we able to contact the primary point of contact for clarification or
315	additional information not provided in this report? (Yes/No)
316	A. [RC] If yes,
317	1. What time, in your local time zone, is the best time to reach you (and/or the
318	primary point of contact)?
319	2. What day of the week is best for us to reach out to the primary point of
320	contact?
321	3. What is the primary point of contact's preferred method of contact? (DESIGN
322	NOTE: Multi select) (Select all that apply) Phone, Email, Other [Describe])
323	(DESIGN NOTE: Open Text)
324	
325	7. [RA] Do you work for the affected entity?
326	A. Not applicable, I am an individual, self-reporting an incident affecting me.
327	B. Yes
328	C. Yes, I am a third party and have been expressly authorized to report on the
329	affected entity's behalf (law firm, incident response firm, etc.) (DESIGN NOTE:
330	Produce this "display note" upon condition the reporter is also reporting pursuant to a reporting
331	requirement >> DISPLAY NOTE: If a third party is submitting a report on behalf of the impacted
332	entity to satisfy another legally required reporting requirement, (1) the third-party submitter must be
333	expressly authorized by the impacted entity to submit reports on its behalf and (2) the other reporting
224 225	requirement must allow for third-party submission of reports. CISA will not verify whether third-
336	entity.)
337	1. [CUIIPlease provide the contact information for the person at the impacted
338	entity who expressly authorized you to report on the entity's behalf.
339	a. [CUI]Name
340	1. First
341	2. Last
342	b [CUIIPhone number(s)
343	1 Preferred
344	2. Alternate
345	c. [CUI] Email address(es) of point of contact
346	1. Preferred
347	2. Alternate
348	d. Job title
349	D. No, I am a third party and do not have the consent and/or have not been expressly
350	authorized to report on the affected entity's behalf (law firm, incident response
351	firm, etc.) (DISPLAY NOTE: If a third party is submitting a report on behalf of the impacted entity
352	without consent and/or authorization, this incident will be validated between the impacted entity and
353	CISA.)
354	

355	g. Impacted Entity Demographics
356	8. [RA] What is the affected entity type?
357	A. Private sector (including U.S. Government contractors)
358	B. U.S. Federal Government agency
359	C. U.S. State, Local, Tribal, or Territorial (SLTT) entity
360	D. Foreign government entity
361	E. Civil society
362	F. Other [describe]
363	9. [RC] (DESIGN NOTE: Applies to only "Private sector" or "Other" selection, except those private sectors
364	that have indicated reporting for a regulatory, statutory, and/or contractual requirement intending to
365	satisfy FISMA and or FedRAMP, then those reporters are directed to Q13 as U.S. Government contractors)
366	Private Sector and Other (DESIGN NOTE: Display the description indicated in Q 8.F "Other"
367	here if applicable) – Impacted Entity Demographics
368	A. Please provide the name of the affected entity. (Please spell out any acronyms.)
369	1. Is the affected entity a subsidiary of a larger entity? (Yes/No) (DESIGN NOTE:
370	If Yes) Provide the name of the larger/parent entity
371	B. Is the affected entity operating in a critical infrastructure sector. ³ ? (Yes/No)
372	1. {Conditional to "Voluntary" report AND "Yes" to "operating a critical
373	intrastructure" AND "Entity Type" is not "Federal Government" (DESIGN
374 375	NOTE: If this is flagged as a "voluntary" report and "yes" as operating a critical infrastructure and NOT a "Federal Government entity" then the following Protected Critical Infrastructure
376	Information (PCII)conditions must be met and asked of the reporter) You have indicated
377	your entity operates in a critical infrastructure sector and is also submitting
378	this report on a voluntary basis. So that your report can be evaluated for
379	protections afforded under the Protected Critical Infrastructure Information
380	(PCII) Program ⁴ , do you consider the information you are sharing to meet
381	any of the following conditions? Select "Yes" if any of the following
382	conditions are true. (Yes/No)
383	a. Is the information, not customarily in the public domain and
384	related to the security of critical infrastructure or protected
385	systems, including documents, records, communication networks,
386	or other information concerning:
387	1. Actual, potential, or threatened interference with, attack on,
388	compromise or incapacitation of critical infrastructure or
389	protected systems by either physical or computer-based attack
390	or other similar conduct that violates Federal, State, local,
391	tribal, or territorial laws, harms interstate commerce of the
392	United States, or threatens public health or safety.

 ³ https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
 ⁴ <u>PCII Program - Frequently Asked Questions | CISA</u> (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

393	2. The ability of any critical infrastructure or protected system to
394	prevent such interference, compromise, or incapacitation;
395	including any planned or past assessment, projection, or
396	estimate of the vulnerability of critical infrastructure or a
397	protected system, including security testing, risk evaluation
398	thereto, risk management planning, or risk audit.
399	3 Any planned or past operational problem or solution regarding
400	critical infrastructure or protected systems including repair
400	entited initiastitucture of protected systems, including repair,
401	recovery, reconstruction, insurance, or continuity, to the
402	extent it is related to such interference, compromise, or
403	incapacitation.
404	b. (DESIGN NOTE: If Yes: DISPLAY NOTE: Thank you. Your submission will be
405	evaluated to ensure it meets the PCII program requirements. Once evaluated and
406	requirements are validated, in order for the PCH protections to be afforded to you for this report you will need to complete and return the "Express and Consent"
407	statement that CISA will send to you via the email contact information you provided.
409	in this form. (DISPLAY NOTE: To learn more about the benefits the PCII
410	program affords qualified submissions please visit, https://www.cisa.gov/resources-
411	tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-
412	program-frequently-asked-questions.))
413	1. If you do not wish to have your submission evaluated as a
414	PCII submission, please check this box []
415	C. (DESIGN NOTE: If No: (DISPLAY NOTE: Thank you. Your submission does not
416	seem to meet the conditions to qualify as protected critical infrastructure
417	information. You may now continue with the rest of the form.)
418	2. (DESIGN NOTE: If Yes) Please select the primary critical infrastructure sector
419	that is impacted by/involved in this incident. If possible, also select the
420	appropriate critical infrastructure-subsector. (DESIGN NOTE: See Appendix 4 for
421	complete critical infrastructure sector and subsector list.)
422	a. Chemical
423	b. Commercial Facilities
424	c. Communications
425	d. Critical Manufacturing
426	e. Dams
427	f. Defense Industrial Base
428	g. Emergency Services
429	h. Energy
430	i. Financial Services
431	j. Food and Agriculture
432	k. Government Facilities
433	1. Healthcare and Public Health
434	m. Information Technology
435	n. Nuclear Reactors, Materials, and Waste
	· · · · ·

436	o. Transportation Systems
437	p. Water and Wastewater Systems
438	q. Unsure
439	3. (DESIGN NOTE: If Yes) Of the 16 listed critical infrastructure sectors, are there
440	any additional critical infrastructure sector(s) with which your organization
441	aligns that were also impacted by the incident? (Yes/No) (DESIGN NOTE: If Yes,
442	Present list of critical infrastructure again and flag as "secondary" critical infrastructure (allow
443	multi select, but all will be flagged as "secondary")) Please select the secondary critical
444	infrastructure sector(s) that is(are) impacted by this incident. If possible, also
445	select the appropriate critical infrastructure critical infrastructure subsector.
446	(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)
447	
448	$10. \ [RC]$ (DESIGN NOTE: Applies to only "U.S. Federal Government agency" selection) U.S. Federal
449	Government agency – Impacted Entity Demographics
450	A. Please provide the Federal agency name (DESIGN NOTE: Select from list in Appendix 5) ⁵
451	1. Please select your sub-agency below after selecting your parent agency (if
452	applicable)(DESIGN NOTE: Select from list in Appendix 5).6)
453	B. We understand all incidents occurring at federal agencies impact the Government
454	facilities critical infrastructure sector ⁷ and it is therefore selected as your primary
455	critical infrastructure. However, are there any additional critical infrastructure
456	sector(s) impacted by the incident occurring at your agency? Please select all that
457	apply. If applicable, also select the appropriate critical infrastructure-subsector.
458	(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.
459	Primary critical infrastructure sector can only be entered once.) (DESIGN NOTE: Flag all Federal
460	Gov entities as "Government facilities" for prime critical infrastructure sector, then allow for one-to-
401	1 Chemical
402	2. Commercial Encilities
405	2. Communications
404	4. Critical Manufacturing
405	4. Critical Manufacturing
400	5. Dallis 6. Defense Industrial Pase
467	6. Defense industrial Base
468	7. Emergency Services
469	8. Energy
4/0	9. Financial Services
471	10. Food and Agriculture
472	11. Government Facilities

⁵ Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)

⁶ Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com) 7 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

473	12. Healthcare and Public Health
474	13. Information Technology
475	14. Nuclear Reactors, Materials, and Waste
476	15. Transportation Systems
477	16. Water and Wastewater Systems
478	17. Unsure
479	C. Of the 16 listed critical infrastructure sectors, are there any additional critical
480	infrastructure sector(s) with which your organization aligns that were also
481	impacted by the incident? (Yes/No) (DESIGN NOTE: If Yes, Present list of critical
482	infrastructure again and flag as "Secondary" critical infrastructure (allow multi select, but all will be
483	flagged as "Secondary")). Please select the secondary critical infrastructure sector(s)
484	that is(are) impacted by this incident. If applicable, also select the appropriate
485	critical infrastructure-subsector. (DESIGN NOTE: See Appendix 4 for complete critical
486	infrastructure Sector and subsector list.)
487	11. [KC] (DESIGN NOTE: Applies to only "U.S. State, local, tribal, or territorial (SLTT) entity" selection)
488	U.S. State, Local, Tribal, or Territorial (SLTT) Entity–Impacted Entity
489	Demographics
490	A. Please provide details about the impacted State, local, tribal, or territorial (SLTT)
491	entity. Select from one of the below SL11 options: (DESIGN NOTE: Single select)
492	I. [] State or territory
493	a. Please provide the impacted entity's name (spell out any
494	acronyms)
495	b. Please select your state or territory below (DESIGN NOTE: Select from
496	list).°
497	
498	2. [] Local
499	a. Please describe your local administrative division (e.g., city,
500	district, county, township, municipality) and the U.S. state or
501	territory your local administrative division is part of:
502	1. Please provide the impacted entity's name (spell out any
503	acronyms)
504	2. Please select the associated state or territory below (DESIGN
505	NOTE: Select from list).9
506	3. [] Tribal
507	a. Tribal governments or communities, please indicate your tribe's
508	name and any U.S. states and/or territories where the tribe is
509	physically located.

⁸ Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com) ⁹ Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All

Items (sharepoint.com)

510	1. Please provide the impacted entity's name
511	2. Please provide the associated U.S. states or territories for
512	reference
513	i. Please select the associated states or territories below
514	(DESIGN NOTE: Select from list). ¹⁰ (DESIGN NOTE: Allow more than
515	one entry as a tribe maybe physically spread across several states and
510	regions) B Is the impacted SLTT Entity in a critical infrastructure sector? ¹¹ (Ves/No)
518	1 Conditional to "voluntary" report AND "Ves" to "operating a critical
510	infrastructure" AND "entity type" is not "Federal Government" (DESICN
520	NOTE: If this is flagged as a "voluntary" report and "Ves" as operating a critical infrastructure
520	and NOT a "Federal Government entity" then the following PCII conditions must be met and
522	asked of the reporter) You have indicated your entity operates in a critical
523	infrastructure critical infrastructure sector and is also submitting this report
524	on a voluntary basis. So that your report can be evaluated for protections
525	afforded under the Protected Critical Infrastructure Information (PCII)
526	Program ¹² , do you consider the information you are sharing to meet any of
527	the following conditions? Select "Yes" if any of the following conditions are
528	true. (Yes/No)
529	a. Is the information, not customarily in the public domain and
530	related to the security of critical infrastructure or protected
531	systems, including documents, records, communication networks,
532	or other information concerning:
533	1. Actual, potential, or threatened interference with, attack on,
534	compromise or incapacitation of critical infrastructure or
535	protected systems by either physical or computer-based attack
536	or other similar conduct that violates Federal, State, local,
537	tribal, territorial laws, harms interstate commerce of the
538	United States, or threatens public health or safety.
539	2. The ability of any critical infrastructure or protected system to
540	prevent such interference, compromise, or incapacitation;
541	including any planned or past assessment, projection, or
542	estimate of the vulnerability of critical infrastructure or a
543	protected system, including security testing, risk evaluation
544	thereto, risk management planning, or risk audit.
545	3. Any planned or past operational problem or solution regarding
546	critical infrastructure or protected systems, including repair,

¹⁰ Use CISA data standards where applicable (<u>Office of the Chief Information Officer - Active Data Standards - All</u> <u>Items (sharepoint.com)</u>

¹¹ https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

 ¹² <u>PCII Program - Frequently Asked Questions | CISA</u> (https://www.cisa.gov/resources-tools/programs/protectedcritical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

547	recovery, reconstruction, insurance, or continuity, to the
548	extent it is related to such interference, compromise, or
549	incapacitation.
550	b. (DESIGN NOTE: If Yes: DISPLAY NOTE: Thank you, Your submission will be
551	evaluated to ensure it meets the PCII program requirements. Once it is evaluated
552	and requirements are validated, you will need to complete and return the "Express
553	and Consent" statement that CISA will send to you via the email contact
554	information you provided in this form in order for the PCII protections to be
555	afforded to you for this report. (DISPLAY NOTE: To learn more about the benefits
556	the PCII program affords qualified submissions please visit,
55/	"https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-
558	information-pen-program/pen-program-frequently-asked-questions".))
559	1. If you do not wish to have your submission evaluated as a DCU submission, plagas shock this have []
560	PCII submission, please check this box []
562	c. (DESIGN NOTE: If No: (DISPLAY NOTE: Thank you, your submission does not
563	information. You may now continue with the rest of the form)
505	2 (DESIGN NOTE: KV-) Plags salest the primary critical infrastructure sector
504	2. (DESIGN NOTE: If yes) Flease select the primary critical initiastructure sector $(1 + 1)^{-1}$
565	that is impacted by this incident. If applicable, also select the appropriate
500	critical infrastructure-subsector. (DESIGN NOTE: See Appendix 4 for complete critical
568	intrastructure Sector and subsector list. Primary critical intrastructure Sector can only be
560	1 Chemical
570	2. Commercial Facilities
571	3. Communications
572	4 Critical Manufacturing
572	5 Dams
574	6. Defense Industrial Base
575	7. Emergency Services
576	8. Energy
577	9. Financial Services
578	10. Food and Agriculture
579	11. Government Facilities
580	12. Healthcare and Public Health
581	13. Information Technology
582	14. Nuclear Reactors, Materials, and Waste
583	15. Transportation Systems
584	16. Water and Wastewater Systems
585	3. (DESIGN NOTE: If Yes) Of the 16 listed critical infrastructure sectors, are there
586	any additional critical infrastructure sector(s) with which your entity aligns
587	that were also impacted by the incident? (Yes/No) (DESIGN NOTE: If Yes, present
588	list of critical infrastructures again and flag as "secondary" critical infrastructure (allow multi
589	select, but all will be flagged as "secondary") Please select the secondary critical
590	infrastructure sector(s) that is(are) impacted by this incident. If applicable,

591	also select the appropriate critical infrastructure subsector. (DESIGN NOTE: See
592	Appendix 4 for complete critical infrastructure Sector and Subsector list.)
593	
594	12. [RC] (DESIGN NOTE: Applies to only "Foreign Government Entity" selection) Foreign
595	Government Entity – Impacted Entity Demographics
596	A. Please provide details about the impacted foreign entity
597	1. Please select your country below (select from list) 13
598	2. Please provide the impacted entity's name (spell out any acronyms)
599	3. Is your entity a computer security incident response team (CSIRT)? (Yes/No)
600	a. (DESIGN NOTE: If Yes, show question) Please enter the name of the
601	CSIRT (DESIGN NOTE: Open text)
602	B. Is the impacted entity in a critical infrastructure sector. ¹⁴ (based on U.S.
603	designation) (Yes/No)
604	a. (DESIGN NOTE: If Yes) Please select the primary critical infrastructure
605	sector that is impacted by this incident. If applicable, also select
606	the appropriate critical infrastructure-subsector. (DESIGN NOTE: See
607	Appendix 4 for complete critical infrastructure sector and subsector list. Primary
608	critical infrastructure sector can only be entered once.)
609	1. Chemical
610	2. Commercial Facilities
611	3. Communications
612	4. Critical Manufacturing
613	5. Dams
614	6. Defense Industrial Base
615	7. Emergency Services
616	8. Energy
617	9. Financial Services
618	10. Food and Agriculture
619	11. Government Facilities
620	12. Healthcare and Public Health
621	13. Information Technology
622	14. Nuclear Reactors, Materials, and Waste
623	15. Transportation Systems
624	16. Water and Wastewater Systems
625	17. Unsure
626	b. (DESIGN NOTE: If Yes) Of the 16 listed critical infrastructure sectors,
627	are there any additional critical infrastructure sector(s) with which
628	your entity aligns that were also impacted by the incident?

 ¹³ Use CISA data standards where applicable (<u>Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)</u>
 ¹⁴ https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

629	(Yes/No/Unsure) (DESIGN NOTE: If Yes, present list of critical
630	infrastructures again and flag as "secondary" critical infrastructure (allow multi
631	select, but all will be flagged as "secondary") Please select the secondary
632	critical infrastructure sector(s) impacted by this incident. If
633	applicable, also select the appropriate critical infrastructure-
634	subsector. (DESIGN NOTE: See Appendix 4 for complete critical infrastructure
635	sector and subsector list.)
636	13. [RC] (DESIGN NOTE: applies to only "FISMA and/or FEDRAMP" regulatory selection plus "private
637	sector" organization type "aka entity is a U.S. Federal Government contractor") U.S. Federal
638	Government Contractor – Impacted Entity Demographics
639	A. Please provide the impacted Federal agency you are supporting (DESIGN NOTE:
640	Select from list in Appendix 5). ¹⁵
641	1. Please select the sub-agency below, if applicable) (DESIGN NOTE: Select from list
642	in Appendix 5). ¹⁶
643	B. We understand that all incidents occurring at federal agencies impact the
644	government facilities critical infrastructure sector and have therefore selected it as
645	your primary critical infrastructure sector. Are there any additional critical
646	infrastructure sector(s) impacted by the incident occurring at your agency? Please
647	select all that apply. If applicable, also select the appropriate critical
648	infrastructure-subsector.
649	a. (DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and
650 651	subsector list. Primary critical infrastructure sector can only be entered once.) (DESIGN NOTE: Flag all Federal Gov entities as "government facilities" as their
652	prime critical infrastructure sector, then allow for one-to-many secondary critical
653	infrastructure sectors and sub sectors.)
654	1. Chemical
655	2. Commercial Facilities
656	3. Communications
657	4. Critical Manufacturing
658	5. Dams
659	6. Defense Industrial Base
660	7. Emergency Services
661	8. Energy
662	9. Financial Services
663	10. Food and Agriculture
664	11. Government Facilities
665	12. Healthcare and Public Health
666	13. Information Technology
667	14. Nuclear Reactors. Materials. and Waste

¹⁵ Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com) ¹⁶ Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All

Items (sharepoint.com)

668	15. Transportation Systems
669	16. Water and Wastewater Systems
670	17. Unsure
671	b. Of the 16 listed critical infrastructure sectors, are there any
672	additional critical infrastructure sector(s) with which your
673	organization aligns that were also impacted by the incident?
674	(Yes/No/Unsure) (DESIGN NOTE: If Yes, Present list of critical
675	infrastructures again and flag as "secondary" critical infrastructure (allow multi
676	select, but all will be flagged as "secondary") Please select the secondary
677	critical infrastructure sector(s) impacted by this incident. If
678	applicable, also select the appropriate critical infrastructure-
679	subsector. (DESIGN NOTE: See Appendix 4 for complete critical infrastructure
680	sector and subsector list.)
681	C. [Fed Ctr] Please enter the contract number(s), clearance level (contract and
682	facility), and prime contractor information and points of contact that correspond
683 684	to the primary contract impacted by or involved in this incident. (DESIGN NOTE:
685	and repeat the following as necessary for each contract entered)
686	1. Contract number(s)
687	2. Contract or other agreement clearance level
688	a. Unclassified
689	b. Confidential
690	c. Secret
691	d. Top Secret
692	e. Not Applicable
693	3. [Fed Ctr] Has the impacted entity been granted a facility security clearance?
694	(Yes/No)
695	a. (DESIGN NOTE: If Yes) [Fed Ctr] What is the facility clearance level
696	(FCL) of the impacted entity?
697	1. Unclassified
698	2. Confidential
699	3. Secret
700	4. Top Secret (may or may not include Sensitive Compartmented
701	Information)
702	5. Not applicable
703	4. [Fed Ctr] Are you the prime contractor under this contract? (Yes/No)
704	a. (DESIGN NOTE: If N_0) Please provide the prime contractor point of
705	contact
706	1. Name
707	i. First
708	ii. Last

709	2. Phone number(s)
710	3. Email address(es)
711	4. Position/title
712	5. Address
713	i. Street name and number
714	ii. Postal code
715	iii. City
716	iv. State
717	v. Country
718	vi. Time zone
719	5. [Fed Ctr] Please provide your US government contracting point(s) of contact
720	(DISPLAY NOTE: Examples of possible US government contracting points of contact are
721	typically the Contracting Officer (CO), Contracting Officer Representative (COR), US
/22	Government Administrative Contracting Officer (ACO). ¹⁷ and US Government Program
723	Manager (PM).) (DESIGN NOTE: Allow for more than one entry)
724	
725	1. First
/26	2. Last
727	b. Phone number(s)
728	c. Email address(es)
729	d. Position/title ¹⁸ (e.g., CO, COR, ACO, PM) (DESIGN NOTE: Provide
/30	"dropdown list" to select from example list, allow "OTHER" with a fill-in
731	e Address
732	1 Street name and number
733	2 Postal code
734	2. Fistal code
755	J. State
730	4. State
/3/	J. Country
/38	6. Time zone
739	
740	14. [RC] (DESIGN Note: Applies to only "civil society" selection) Civil Society – Impacted Entity
741	Demographics
742	A. Please provide details about the impacted civil society entity

 ¹⁷ <u>48 CFR § 842.271 - Administrative Contracting Officer's role in contract administration and delegated functions.</u>]
 <u>Electronic Code of Federal Regulations (e-CFR)</u> US Law | LII / Legal Information Institute (cornell.edu)
 ¹⁸ DESIGN NOTE: for each Position selected provide "DISPLAY NOTE" as appropriate:

CO – person who has authority over the contract and ability to direct contractor activities; COR - POCs could be a federal employee who has authority and ability to direct contractor activities; ACO - Unless you are supporting the VA or DOD it is unlikely that you have an ACO; PM – person overseeing the technical effort and has the authority to direct contractor activities.)

743	1. Please describe your organization's sector within civil society (e.g.,
744	academia, faith-based, think tank, media, advocacy, political party, labor
745	union) (DESIGN NOTE: Open text)
746	2. Please enter the civil society entity's name (spell out any acronyms)
747	B. Are there any critical infrastructure (critical infrastructure) sector(s). ¹⁹ directly
748	impacted by the incident that occurred/is occurring at your organization?
749	(Yes/No)
750	1. {Conditional to "voluntary" report AND "Yes" to "operating a critical
751	infrastructure" AND "entity type" is not "Federal Government"} (DESIGN
752	NOTE: If this is flagged as a "voluntary" report and "Yes" as operating a critical infrastructure
753	and NOT a "Federal Government entity" then the following PCII conditions must be met and
754	asked of the reporter) if ou have indicated your entity directly impacts a critical
755	So that accurate and is also submitting this report on a voluntary basis.
756	So that your report can be evaluated for protections afforded under the
/5/	Protected Critical Infrastructure Information (PCII) Program ⁻¹ , do you
758	consider the information you are sharing to meet any of the following
759	conditions? Select "Yes" if any of the following conditions are true. (Y = 0.1)
760	(Yes/No)
761	a. Is the information, not customarily in the public domain and
762	related to the security of critical infrastructure or protected
763	systems, including documents, records, communication networks,
764	or other information concerning:
765	1. Actual, potential, or threatened interference with, attack on,
766	compromise or incapacitation of critical infrastructure or
767	protected systems by either physical or computer-based attack
768	or other similar conduct that violates Federal, State, local,
769	tribal, territorial laws, harms interstate commerce of the
770	United States, or threatens public health or safety.
771	2. The ability of any critical infrastructure or protected system to
772	prevent such interference, compromise, or incapacitation;
773	including any planned or past assessment, projection, or
774	estimate of the vulnerability of critical infrastructure or a
775	protected system, including security testing, risk evaluation
776	thereto, risk management planning, or risk audit.
777	3. Any planned or past operational problem or solution regarding
778	critical infrastructure or protected systems, including repair,
779	recovery, reconstruction, insurance, or continuity, to the

 ¹⁹ https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
 ²⁰ <u>PCII Program - Frequently Asked Questions | CISA</u> (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

780	extent it is related to such interference, compromise, or
781	incapacitation.
782 783 784 785 786 787 788 789 790	b. (DESIGN NOTE: If Yes: DISPLAY NOTE: Thank you. Your submission will be evaluated to ensure it meets the PCII program requirements. Once it is evaluated and requirements are validated, you will need to complete and return the "Express and Consent" statement that CISA will send to you via the email contact information you provided in this form in order for the PCII protections to be afforded to you for this report. (DISPLAY NOTE: To learn more about the benefits the PCII program affords qualified submissions please visit, "https://www.cisaa.gov/resources-tools/programs/protected-critical-infrastructure- information-pcii-program/pcii-program-frequently-asked-questions".))
791	1. If you do not wish to have your submission evaluated as a
792	PCII submission, please check this box []
793	
794 795 796 797	c. (DESIGN NOTE: If No: (DISPLAY NOTE: Thank you. Your submission does not seem to qualify as protected critical infrastructure information. You may now continue with the rest of the form.)
798	2 (DESIGN NOTE: If Ves) Please select all critical infrastructure sectors impacted
799	by this incident. If applicable, also select the appropriate critical
800	infrastructure-subsector. (DESIGN NOTE: Multi select) (DESIGN NOTE: See Appendix 4
801	for complete critical infrastructure sector and subsector list.)
802	a. Chemical
803	b. Commercial Facilities
804	c. Communications
805	d. Critical Manufacturing
806	e. Dams
807	f. Defense Industrial Base
808	g. Emergency Services
809	h. Energy
810	i. Financial Services
811	j. Food and Agriculture
812	k. Government Facilities
813	1. Healthcare and Public Health
814	m. Information Technology
815	n. Nuclear Reactors, Materials, and Waste
816	o. Transportation Systems
817	p. Water and Wastewater Systems
818	q. Unsure
819	15. [Op] + [FISMA Req] What is the primary website of the impacted entity?
820	16. [Op] + [FISMA Req] Please enter the impacted entity's internal tracking number(s)
821	related to this incident, (e.g. case number), if applicable. (DESIGN NOTE: if "N/A" is
822	selected, internal tracking number can be blank)

823	A. Not applicable (DESIGN NOTE: Radio button)
824	B. Internal tracking number(s) (DESIGN NOTE: Text box)
825	17. [Op] + [RR] If applicable, provide the primary location and/or facility address where
826	this incident or event occurred. (If applicable, you can also add secondary locations).
827	A. (DESIGN NOTE: Allow one to many entries. Flag all but first entry as "secondary" addresses of the
828	impacted entity.)
829	1. Not applicable (DESIGN NOTE: Radio button - Allow to bypass "address info" if not
830	applicable is selected)
831	2. Name of primary (secondary if applicable) location (e.g., building name,
832	pipeline designation, data center, shipping port, airport, telecom site, etc.) if
833	applicable. (DESIGN NOTE: Open text and allow "not applicable" as selection option for
834	name. Also, either address info should be entered, or the latitude and longitude of the location
835	should be entered. both could be allowed, but at least one location designation should be
836	required)
837	5. Street name and number
838	4. City
839	5. State
840	6. Postal code
841	7. Country 2^{1}
842	B. If the incident occurred in a location without a known address, please provide the
843	coordinates (latitude and longitude) to the best of your ability for the location of
844	the incident. (DISPLAY NOTE: Many critical infrastructure sector facilities, such as cellular
845	towers in the communications sector or offshore oil platforms in the oil and natural gas (ONG)
840 847	subsector, do not nave street addresses. Understanding the geographic location can help CISA identify a potential targeting effort by an adversary (DESIGN NOTE: Include an option to enter latitude and
848	longitude with guidance on how to use Google Maps to quickly find the coordinates.)
849	1. Not applicable (DESIGN NOTE: Radio button - Allow to bypass "latitude and longitude
850	info" if not applicable is selected)
851	2. Latitude
852	3. Longitude
853	C Has the incident occurred on or involved a movable entity (e.g., ship, aircraft
854	train)? (Ves/No)
855	1 (DESIGN NOTE: If Ves) Please describe the entity that was involved in this
856	incident (DESIGN NOTE: Onen text)
857	18 [On] + [RR] Please provide the following information about the impacted
858	organization (Answer for the impacted entity and not the parent entity)
850	Δ Do you know if the impacted entity that owns and/or operates the facility (ies)
860	where the incident occurred has any unique government or business
000	identifiers (e.g. North American Industrial Classification System (NAICS)
90T	idenumers (e.g. norm American industrial Classification System (NAICS),

²¹ Use CISA data standards where applicable (<u>Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)</u>

862	General Services Administration (GSA)-issued Unique Entity Identifier
863	(UEI))? (Yes/No/Unknown)
864	i. [RC] (DESIGN NOTE: If yes) Please select from the identifier(s) below and
865	provide their corresponding numbers: (DESIGN NOTE: Multi select).
866	a. Type of Identifier(s)
867	1. North American Industrial Classification System (NAICS)
868	identifier(s)
869	i. Identifier number(s) (DESIGN NOTE: Repeated for each identifier
870	selected)
871	2. General Services Administration (GSA)-issued Unique Entity
872	Identifier (UEI)
873	3. Environmental Protection Agency FacID
874	4. What are the Commercial and Government Entity (CAGE)
875	Code(s) for the facility location(s) of the impacted system(s)?
876	i. Provide the address of the facility or facilities associated
877	with the CAGE codes. (DISPLAY NOTE: CAGE codes are
878	assigned to suppliers to various government or defense agencies, as well
879	as to government agencies themselves and various organizations. CAGE
880	codes provide a standardized method of identifying a given facility at a
001	specific location.)
882	2. Puilding number (if applicable)
000	2. Suite number (if applicable)
884	5. Suite number (11 applicable)
885	4. City
886	5. State
887	6. Postal code
888	7. Country 22
889	5. Other [please provide the type of identifier]
890	
891	19. [RC] (DESIGN Note: applies only to "Third Party" selection in "red box")
	 [RA] Do you work for the affected entity? A. Not applicable, I am an individual, self-reporting an incident affecting me. B. Yes C. Yes, I am a third party and have been expressly authorized to report on the
892	affected entity's behalf (law firm, incident response firm, etc.) (DESIGN NOTE;
893	You indicated you are a third party authorized to report on behalf of the affected
894	entity. What is the name of your organization? (Please spell out any acronyms)
895	A. Is your organization a subsidiary of a larger organization? (Yes/No)

²² Use CISA data standards where applicable (<u>Office of the Chief Information Officer - Active Data Standards - All</u> <u>Items (sharepoint.com)</u>

896	1. (DESIGN NOTE: If Yes) Provide the name of the larger/parent organization.
897	2. What is the preferred email address of the parent organization (e.g.,
898	soc@organization.gov, soc@organization.com)?
899	3. [Op] What is the primary website of the parent organization?
900	4. [Op] Please enter the parent organization's internal tracking number(s)
901	related to this incident. (e.g., case number), if relevant. (DESIGN NOTE: If "Not
902	applicable" selected, internal tracking number can be blank)
903	a. Not applicable (DESIGN NOTE: Radio button)
904	b. Internal tracking number(s)
905	B. Please provide the following information about your organization. (Please answer
906	for your organization and not any parent organization.)
907	1. What is the preferred email address of your organization?
908	2. What is the primary website of your organization?
909	3. [Op] Please enter the your organization's internal tracking number(s) related
910	to this incident, (e.g., case number), if relevant. (DESIGN NOTE: If "not applicable"
911	is selected, internal tracking number can be blank)
912	a. Not applicable (DESIGN NOTE: Radio button)
913	b. Internal tracking number(s)
914	h.Incident Overview
915	20. [RA] Provide a high-level summary of the incident. (DESIGN NOTE: Open Text) (DISPLAY
916	NOTE: Requests for more details will occur later in this report. Please provide a short "executive
917	summary" of the incident with a narrative of the incident detection. Consider including a description of any
918 919	unauthorized access (including whether the incident involved an unattributed cyber intrusion), identification of any informational impacts or information compromise, any network location where
920	activity was observed, and a high-level description of the impacted system(s) (e.g., "email servers, a network
921	firewall, and a web server").)
922	21. [RA] When was the incident first detected?
923	A. Detection date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
924	22. [RA] Have you performed any incident response activities (e.g., cyber hunt activities)
925	to determine the scope and impact of the incident? (Yes/No)
926	A. {Conditional} [Op] + [FISMA Req] (DESIGN NOTE: If Yes) Please explain and
927	include any actions already taken as well as intelligence you may have learned to
928	date (DESIGN NOTE: Open Text)
929	Incident Category Type Determination
930	23. [RA] To the best of your knowledge, please select the categories involved in this
931	incident (DESIGN NOTE: Multi select, then drop down for more refined selections within each main
932	category, dropdown lists are in Appendix 3.) (DISPLAY NOTE: Select all that apply)
933	A. Malware [e.g., ransomware, DDOS, etc.]
934	B. Human (or technology) errors [e.g., loss of equipment, system misconfiguration,
935	mishandling of sensitive and/or PII documentation, etc.]

936	C. Hacking [e.g., password cracking, SQL injection, cross-site scripting, 'system'
937	overflows, etc.]
938	D. Physical actions/destruction [e.g., sabotage, theft, etc.]
939	E. Environmental factors [e.g., fire, flood, etc.]
940	F. Social engineering [e.g., phishing, extortion, spam, etc.]
941	G. Misuse of assets (sometimes called "insider threats') [e.g., privilege abuse,
942	unauthorized hardware/software, etc.]
943	24. [RA] This incident has led to or resulted in (DESIGN NOTE: Multi select) (DISPLAY NOTE:
944	Select all that apply)
945	A. Classified data "spillage" to unapproved networks
946	B. Compromised system(s)
947	C. Destruction of data or systems (not due to ransomware)
948	D. Destruction of data or systems (via ransomware)
949	E. Defacement
950	F. Equipment loss: loss of control of physical equipment not from theft
951	G. Operational technology response functions inhibited (e.g., safety, protection,
952	quality assurance, and operator intervention functions are prevented from
953	responding to a failure, hazard, or unsafe state ²³)
954	H. Operational technology process control impaired (e.g., physical control processes
955	are manipulated, disabled, or damaged ²⁴)
956	I. Supply chain customer disruption (DISPLAY NOTE: The incident involved one of the
957	reporting entity's vendors, with an impact on the reporting entity)
958	J. Supply chain vendor disruption (DISPLAY NOTE: The incident impacted a system or product
959	that is supplied by the reporting entity to its customers, with a potential impact to one or more
900	K Unauthorized account access
901	K. Unauthorized account access
962	L. Unauthorized removal of account access (e.g., entity's system administrator's
963	
964	IVI. Unauthorized information access
965	N. Unauthorized release of information (virtually via computing systems) ²³

 ²³ Inhibit Response Function, Tactic TA0107 - ICS | MITRE ATT&CK®
 ²⁴ Impair Process Control, Tactic TA0106 - ICS | MITRE ATT&CK®

²⁵ Unauthorized release of information "virtually" is an occurrence where a person other than an authorized user potentially obtains the data, such as by means of a network intrusion, a targeted compromise that exploits website vulnerabilities, the inadvertent disclosure of information (including PII) via a public website, or a phishing or social engineering incident executed through an email message or attachment. It may also include an authorized user obtaining sensitive information (including PII) for other than the authorized purpose. If such an incident involves personally identifiable information (PII) on a federal system, the unauthorized release is considered a Breach per OMB - M-17-12. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII.

966	O. Unauthorized release of information (physically via printed documents or
967	physical media, or orally). ²⁶
968	P. Unauthorized use of information
969	O Other [describe]
505	
970	I. Incident Notifications
971	25. [RA] Have you already notified or reported this incident to an entity other than CISA
972	or do you plan to notify or report this incident to an entity other than CISA? (Yes/No)
973	(DISPLAY NOTE: CISA will not use information reported to fulfill any additional legally required
974	reporting obligations on your or your organization's behalf. Reporting to CISA only satisfies legally
975	required reporting requirements to the extent that the reporting requirement explicitly provides that
977	A [CUI]{Conditional} [FISMA Reg] (DESIGN NOTE: If Yes) Please list the entities you
978	will, or did, report to.
979	1. Information owners (including information managed by the
980	affected/reporting entity (e.g., cloud provider), and information owned by the
981	affected/reporting entity's customer/client agency (e.g., customer owned
982	information managed by a contracted 3 rd party) (DESIGN NOTE: Repeat the
983	following for each notification entity selected, can also be more than one entry per category, e.g.,
984	law enforcement can be local and federal notifications)
985	a. Entity Details (Design Note: Provide check box to allow the reporter to identify
986 987	if this value is the same as the impacted entity's name. If box is checked, copy the impacted entity's name to this variable)
988	1. Organization Name
989	2. [CUI]Point of contact name
990	i. First
991	ii. Last
992	3. Email address(es) of Point of Contact
993	4. Phone number(s)
994	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
995	offset>)
996	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
997	<utc offset="">)</utc>
998	d. Case/incident/report number provided (if applicable)
999	2. Inspector general (DESIGN NOTE: Repeat the following sub entries "a through d" for each
1000	notification entity selected, other than the information owner. There can also be more than one
1001	entry "a through d" per category, e.g., law enforcement can be local and federal.)
1002	a. Entity Details

 $^{^{26}}$ Unauthorized release of information "physically" is an occurrence where a person other than an authorized user potentially obtains the data due to the loss or theft of physical documents that include information (including PII), portable electronic storage media that stores information (including PII), or an oral disclosure of this sensitive information (including PII) to a person who is not authorized to receive that information. If such an incident involves PII on a federal system, the unauthorized release is considered a Breach per OMB – M-17-12. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device. This result includes improper disposal of sensitive and/or PII documentation in containers that could be accessed by nonauthorized personnel (e.g., information with customer credit card or social security numbers thrown in local dumpster or lost mail containing PII).

1003	1. Organization Name
1004	2. [CUI]Point of contact name
1005	i. First
1006	ii. Last
1007	3. Email address(es) of Point of Contact
1008	4. Phone number(s)
1009	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1010	offset>)
1011	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1012	<utc offset="">)</utc>
1013	d. Case/incident/report number provided (if applicable)
1014	3. Legal counsel
1015	4. Law enforcement
1016	5. Regulatory agency
1017	6. Privacy officials
1018	7. Security staff
1019	8. System owners
1020	9. Other (DESIGN NOTE: Repeat the following sub entries a through d for each notification
1021	entity selected, other than the information owner. There can also be more than one entry "a through d" ner category, e.g., law enforcement can be local and federal.)
1023	a. Entity Details
1024	1. Organization Name
1025	2. [CUI]Point of contact name
1026	i. First
1027	ii. Last
1028	3. Email address(es) of Point of Contact
1029	4. Phone number(s)
1030	5. Position/Title
1031	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1032	offset>)
1033	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1034	<utc offset="">)</utc>
1035	d. Case/incident/report number provided (if applicable)
1036	
1037	B. [CUI] {Conditional} [FISMA Req] (DESIGN NOTE: If Yes) Have you already, or are
1038	you planning to report this incident to any federal government agency other than
1039	CISA?
1040	1. [If Yes] Which agency? (DESIGN NOTE: Select from agency list in Appendix 5)
1041	a. Entity Details (Design Note: Provide check box to allow the reporter to identify if this value is the same as the imported entity's name. If here is checked easy the
1042	impacted entity's name to this variable)
1044	1. Organization Name
1045	2. [CUI]Point of contact name
1046	i. First
1047	ii. Last
1048	3. Email address(es) of Point of Contact
1049	4. Phone number(s)

1050	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< th=""></utc<>
1051	offset>)
1052	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1053	<utc offset="">)</utc>
1054	d. Case/incident/report number provided (if applicable)
1055	C. (DESIGN NOTE: All other reporters not FISMA) [CUI] {Conditional} [Op] (DESIGN NOTE:
1056	If Yes) Please list the entities you will, or did, report to. (DISPLAY NOTE: This
1057	information may be helpful for CISA to understand if there are other entities that CISA may need to
1058	collaborate with or allow for special considerations during any incident response efforts.)
1059	1. Information owners (examples include information managed by
1060	affected/reporting entity (e.g., cloud provider) but owned by
1061	affected/reporting entity's customer/client) (DESIGN NOTE: Repeat the following for
1062	each notification entity selected, can also be more than one entry per category, e.g., law
1005	enforcement can be local and lederal notifications.)
1064	a. Entity Details (Design Note: Provide eneck box to allow the reporter to identify if this value is the same as the impacted entity's name. If hox is checked, convitte
1066	impacted entity's name to this variable)
1067	1. Organization Name
1068	2. [CUI]Point of contact name
1069	i. First
1070	ii. Last
1071	3. Email address(es) of Point of Contact
1072	4. Phone number(s)
1073	b. Already notified: Date and time (vvvv-mm-dd HH:MM - <utc< td=""></utc<>
1074	offset>)
1075	c. Plan to notify: Date and approximate time (vvvv-mm-dd HH:MM -
1076	<utc offset="">)</utc>
1077	d. Case/incident/report number provided (if applicable)
1078	2. Law enforcement (DESIGN NOTE: Repeat the following sub entries a through d for each
1079	notification entity selected, other than the information owner. There can also be more than one
1080	entry "a through d" per category, e.g., law enforcement can be local and federal.)
1081	a. Entity Details
1082	1. Organization Name
1083	2. [CUI]Point of contact name
1084	i. First
1085	ii. Last
1086	3. Email address(es) of Point of Contact
1087	4. Phone number(s)
1088	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1089	offset>)
1090	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1091	<utc offset="">)</utc>
1092	d. Case/incident/report number provided (if applicable)
1093	3. Regulatory agency
1094	4. Other federal agencies
1095	a. If selected, which agency? (DESIGN NOTE: Select from agency list in
1096	Appendix 5)

1097	5. Other (DESIGN NOTE: Repeat the following sub entries a through d for each notification
1098	entity selected, other than the information owner. There can also be more than one entry "a
1099	through d" per category, e.g., law enforcement can be local and federal.)
1100	a. Entity Details
1101	1. Organization Name
1102	2. [CUI]Point of contact name
1103	i. First
1104	ii. Last
1105	3. Email address(es) of Point of Contact
1106	4. Phone number(s)
1107	5. Position/Title
1108	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1109	offset>)
1110	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1111	<utc offset="">)</utc>
1112	d. Case/incident/report number provided (if applicable)
1113	j. Incident: Severity Assessments
1114	Confidentiality, Integrity, Availability (CIA) Assessment ²⁷

1115	26. [RA] (DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event-
1116	Incident FLAG for FISMA reporters only. If Q26 A-C are answered "no", that terminates the rest of the
1117	Incident Questions for a FISMA reporter, and the FISMA reporter is directed towards filling out "Event
1118	Reporting" only.) At this time, is this incident known to either imminently ²⁸ or actually
1119	jeopardize, without lawful authority, any of the following relating to either
1120	information or an information system? (select all that apply) (DESIGN NOTE: For non-
1121	FISMA reports, if "unsure/None" selected for all three CIA questions, then DISPLAY NOTE: You have not
1122	indicated an impact on at least one of the three areas of confidentiality, integrity, or availability per the
1123	definition of an incident.)
1124	A. Confidentiality ²⁹ [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Have

radio button for all)

1125

²⁷ The concepts of confidentiality, integrity, and availability (CIA), often referred to as the "C-I-A triad," represent the three pillars of information security. See, e.g., NIST, NIST Special Publication 1800-25 Vol. A, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, at 1 (Dec. 2020), available at https://csrc.nist.gov/pubs/sp/1800/25/final

²⁸ Imminently: [a. Imminent] "ready to take place; happening soon" or " something bad or dangerous seen as menacingly near." [b. Imminent danger] "[Such an appearance of threatened and impending injury [could change to harm to an entity's information or information systems] as would put a reasonable and prudent [person] to his instant defense." Specifically surrounding networks and data imminently implies there is reasonable suspicion a threat is going to target my entity's information or information systems. [derived from a. Webster's Dictionary and b. Black's Law Dictionary {respectively}]

²⁹ "Confidentiality" refers to "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." [e.g., threat actor has access to your information or an information system, without consent.]

1126 1127	B. Integrity, ³⁰ [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Have radio button for all)
1128	C. Availability. ³¹ [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Have
1129	radio button for all)
1130	
1131	Violation of Law and Policy
1132	27. [RA] At this time, does this incident constitute an imminent or actual violation of law,
1133	security policies, security procedures, or acceptable use policies? (Yes/No) (DESIGN
1134	NOTE: If Yes) Please make selection(s) below
1135	A. Violation of law [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Single
1136	select have radio button for all.)
1137 1138	B. Security policies and/or procedures [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Single select have radio button for all.)
1139	C. Acceptable use policies [] imminently; [] actually; [] unsure; [] none (DESIGN
1140	NOTE: Single select have radio button for all.)
1141	
1142	Incident: High-Level Impacts
1143	Public Impacts
1144	National US Impacts
1145	(DESIGN NOTE: Major Incident Flag Questions. Any "Yes" answer here is used to determine if the reporter is
1146	reporting a major incident as defined by FISMA in the next question by adding in "Demonstrable Harm" for
1147	those that selected "Yes" here.)
1148	28. $[Op] + [FISWA Req] 10$ the best of your knowledge, does the incident likely impact
1149	any of the following? (Select all that apply)
1150	A. National security interests of the United States
1151	B. Foreign relations of the United States
1152	C. Economy of the United States
1153	D. Public confidence of the American people
1154	E. Civil liberties of the American people
1155	F. Public health and safety of the American people
1156	(DESIGN NOTE: Major Incident - FLAG Questions: For "Q29" question, users should see all options from "Q
1157	28 that they selected., "the incident is likely to result in any impact to" above for which the answer was selected. This is a distinction for FISMA reports only) (DISPLAY NOTE: Any impacts selected with a "demonstrable
1159	harm" severity, will indicate that the incident is considered a major incident" under FISMA reporting.)
1160	29. [Op] + [FISMA Req] At the time of this report, of the likely impacts of this incident
1161	selected above, are any of them likely to result in demonstrable harm to the United
1162	States? (DISPLAY NOTE: Select those that are likely to result in demonstrable harm.) (DESIGN NOTE:
1163	Skip this question if nothing selected in question 28. Display list containing only the options the user

³⁰ "Integrity" refers to "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity." [e.g., a threat actor has modified or deleted your information, without your consent.]

consent.] ³¹ "Availability" refers to "ensuring timely and reliable access to and use of information." [e.g., a threat actor has impeded you from accessing or operating the information system or information in the way you intended (DDOS)]

1164 1165	selected in Q28. Provide user a "check box" in Q29 so they can indicate which options represent "demonstrable harm.")
1166	Regional Impacts (Local to Global)
1167	30. $[Op] + [RR]$ To the best of your knowledge, describe the extent of the incident's
1168	impact on the population/geographic region
1169	A. Internal/site-specific (Impacts are felt by the impacted entity or a particular
1170	facility or site, but not externally)
1171	B. Local (Impact is limited to entities or customers in the immediate area (e.g., town,
1172	city) external to the core business of the affected entity)
1173	C. State/territory-wide
1174	D. Regional
1175	E. Multi-regional
1176	F. National
1177	G. Multi-national
1178	H. Global
1179	I. Unknown
1180	
1181	Breach. ³² Severity Impacts
1182	31. [Op] + [FISMA Req] At this time, has the incident resulted in any confirmed
1183	unauthorized access to personally identifiable information? (Yes/No) (DESIGN NOTE: If
1184	Yes, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions
1185	"access due" and "accessed by" only if "Yes".)
1100	A. Was the access due to (select all that apply).
1107	2. Compromise
1100	2. Unauthorized disclosure
1109	4. Unauthorized acquisition
1101	B Was the information accessed by (select all that apply):
1102	1. A person other than an authorized user
1102	2 An authorized user who accessed the personally identifiable information for
110/	an other-than-authorized purpose
1105	32 {Conditional}[On] + [FISMA Rea] (DESIGN NOTE: Do not ask this question if the "Confirmed
1196	Unauthorized Access" question yields a positive selection response. Only ask in previous response to
1197	"confirmed" = "No") At this time, has the incident resulted in any potential unauthorized
1198	access to personally identifiable information? (Yes/No) (DESIGN NOTE: If Yes, flag as
1199	Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access
1200	due" and "accessed by" only if "Yes".)
1201	A. Was the potential unauthorized access due to: (select all that apply)

³² Breach: "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other-than-authorized purpose." per OMB M-17-12

1202	1. Loss of control
1203	2. Compromise
1204	3. Unauthorized disclosure
1205	4. Unauthorized acquisition
1206	B. Was the information potentially accessed by (select all that apply)
1207	1. A person other than an authorized user
1208	2. An authorized user who accessed the personally identifiable information for
1209	an other-than-authorized purpose
1210	(DESIGN NOTE: Following responses for Q31 and Q32, if breach severity "confirmed or potential unauthorized
1211 1212	access" = Yes, DISPLAY on "POP UP SCREEN", display note to reporter: "You have indicated you have had an actual or potential breach and impacts to PIL. You will be given an opportunity to provide more details on the
1213	types of PII impacted later in this report.")
1214	Major Incident Severity Determination (FISMA Only)
1215	33. [FISMA Req] At the time of this report, did any of the following occur involving
1216	personally identifiable information? (DESIGN NOTE: Major Incident - FLAG Question: Only
1217	appears if Breach Severity "Confirmed or Potential Unauthorized Access" = Yes. If any "100,000" field is
1218	answered yes below, hag as major incident. (DESIGN NOTE: a FISMA major incident = a significant cyber incident) (DESIGN NOTE: multi select) (DISPLAY NOTE: Select all that apply)
1220	A. [] Unauthorized modification
1221	1. (DESIGN NOTE: If selected display following:)
1222	a. Was this a [] potential or [] actual occurrence?
1223	b. Did this occurrence or potential occurrence involve the PII of
1224	100,000 or more people? (Y/N)
1225	B. [] Unauthorized deletion
1226	1. (DESIGN NOTE: If selected display following:)
1227	a. Was this a [] potential or [] actual occurrence?
1228	b. Did this occurrence or potential occurrence involve the PII of
1229	100,000 or more people? (Y/N)
1230	C. [] Unauthorized exfiltration
1231	1. (DESIGN NOTE: If selected display following:)
1232	a. Was this a [] potential or [] actual occurrence?
1233	b. Did this occurrence or potential occurrence involve the PII of
1234	100,000 or more people? (Y/N)
1235	D. [] Unauthorized access
1236	1. (DESIGN NOTE: If selected display following:)
1237	a. Was this a [] potential or [] actual occurrence?
1238	b. Did this occurrence or potential occurrence involve the PII of
1239	100,000 or more people? (Y/N)
1240	34. [FISMA Req] At the time of this report, has your answer to any item within the
1241	preceding "major incident severity" questions changed since a previous report?
1242	$(\mathrm{Yes/No})$ (DESIGN NOTE: Only show if "supplemental/update" or "post-incident" report is selected)
1243	A. (DESIGN NOTE: If Yes) Did this change cause the report to (Select one response)
1244	1. [] Upgrade to a major incident?

1245	a. Please provide additional context for the change
1246	2. [] Downgrade from a major incident?
1247	a. Please provide additional context for the change
1248	3. [] No change in major incident determination (the incident was either
1249	previously not determined to be a major incident and remains as such, or was
1250	previously determined to be a major incident and remains as such)
1251	a. Please provide additional context
1252	$35. \ [FISMA Req]$ (DESIGN NOTE: Only asked of FISMA reporters if the incident has been indicated as a
1253	"Major Incident" per thresholds in questions 29 and/or 33.) Has this incident been reported to
1254	Congress? (Yes/No)
1255	Public Health and Safety Impacts
1256	36. [Op] + [RR] To the best of your knowledge, what is the current impact of this
1257	incident on public health? (DISPLAY NOTE: Public health impacts are defined as "impacts on an
1258	affected population measured based on new and increased death, disease, injury, and disability." Impacts to
1259	access to medical care are considered public safety impacts, which are addressed in a later question.)
1260	A. No impact – Incident has no impact on public health
1261	B. Low impact – Incident has resulted in one or more minor injuries and/or
1262	temporary disabilities that have not required emergency response (e.g., minor
1263	symptoms prompting self-care)
1264	C. Moderate impact – Incident has resulted in one or more moderate injuries and/or
1265	lasting disabilities that have required emergency response and/or risk (e.g., easily
1266	treated symptoms or hospital diagnostic visits)
1267	D. High impact – Incident has resulted in one or more serious injuries that have
1268	required emergency response and/or permanent disabilities
1269	E. Critical impact – Incident has resulted in one or more deaths
1270	F. Unknown impact – Reporter does not have information required to assess the
1271	impact of the incident on public health
1272	37. [Op] + [RR] To the best of your knowledge, what is the current impact of this
1273	incident on public safety? (DISPLAY NOTE: Public safety impacts are defined as "Impact measured
1274	based on an affected population's ability to obtain shelter (e.g., temporary housing, temperature
1275	regulation), healthcare (e.g., emergency response services, open hospital beds), and lifeline resources (e.g.,
1270	physical safety (e.g., data breaches that threaten individual safety).")
1278	A. No impact – Incident has no impact on public safety
1279	B. Low impact – Incident has minimal impact on public safety (e.g., limited, short
1280	term disruption of essential services and/or lifeline resources – phone and internet
1281	service, electricity, water)
1282	C. Moderate impact – Incident has more extensive impact on public safety (e.g.,
1283	longer-term disruption of lifeline resources such as phone, internet, electricity.
1284	and water; healthcare and shelter impacts/disruptions from loss of electricity for
1285	extended period)
1205	extended period)

1286	D. High impact – Incident has severe impact on public safety (e.g., evacuation and
1287	temporary housing of displaced communities; immediate threats to physical safety
1288	of the public; extended disruption of essential services; stress on healthcare
1289	resources; water and air contamination)
1290	E. Critical impact – Incident has catastrophic impact on public safety (e.g., long-term
1291	environmental contamination; cessation of essential services such as law
1292	enforcement and healthcare; societal instability)
1293	F. Unknown impact – Reporter does not have the information required to assess the
1294	impact of the incident on public safety
1295	Indirect Impacts
1296	38. [Op] + [RR] To the best of your knowledge, were/are there any indirect (or
1297	secondary) impacts to other critical infrastructure sector(s) ³³ ? (Yes/No)
1298	A. (DESIGN NOTE: If Yes) Please select the appropriate critical infrastructure sector and
1299	the appropriate critical infrastructure subsector(s) (if applicable) that were
1300	indirectly impacted, and indicate what type of impact (functional, informational,
1301	economic and/or physical). (DESIGN NOTE: See Appendix 4 for complete critical
1302	infrastructure sector and subsector list.)
1303	(DESIGN NOTE: Multi select) (DISPLAY NOTE: Indirect impact is defined as "an effect that is not a
1304	direct consequence of an incident, but is caused by a direct consequence, subsequent cascading effects,
1305	and/or related decisions. For example, if an electric power plant is the victim of a malicious cyber incident,
1306	directly impacting the provision of energy sector services (in this case, electricity), other local or regional
1307	sectors that are dependent on that electricity – e.g., commercial facilities and critical manufacturing – may
1308	experience indirect impacts.")
1309	1. Chemical (DESIGN NOTE: Multi select include any subsector lists from Appendix 4 as
1310	necessary and repeat the four "impact" selections per critical infrastructure-cross sector and/or
1311	subsector instance selected)
1312	a. Type(s) of Impact: (DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all
1313	that apply)
1314	1. Functional impact. ³⁴
1315	2. Informational impact ³⁵
1316	3. Economic impact ³⁶

 ³³ https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
 ³⁴ Functional impact: A measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), little or no impact may be experienced due to the incident (CISA National Incident Cyber Scoring System). <u>CISA National Cyber Incident Scoring System (NCISS) | CISA</u>

³⁵ **Informational Impact**: In addition to functional impact, incidents may also affect the confidentiality, integrity and availability of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. (CISA National Incident Cyber Scoring System). <u>CISA National Cyber Incident Scoring System (NCISS) | CISA</u>

³⁶ Economic Impact: Any costs or losses experienced due to an incident, including the general categories listed in this form in question #38A-G. These categories are more specifically defined in the CISA report: "Cost of Cyber Incident;" see Table 44 in Appendix C, <u>https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf</u>

1317	4. Physical impact ³⁷
1318	b. Subsector list (if available) here: (DESIGN NOTE: Multi select) (DISPLAY
1319	NOTE: Select all that apply)
1320	1. Type(s) of Impact:
1321	i. Functional impact
1322	ii. Informational impact
1323	iii. Economic impact
1324	iv. Physical impact
1325	2. Commercial Facilities
1326	3. Communications
1327	4. Critical Manufacturing
1328	5. Dams
1329	6. Defense Industrial Base
1330	7. Emergency Services
1331	8. Energy
1332	9. Financial Services
1333	10. Food and Agriculture
1334	11. Government Facilities
1335	12. Healthcare and Public Health
1336	13. Information Technology
1337	14. Nuclear Reactors, Materials, and Waste
1338	15. Transportation Systems
1339	16. Water and Wastewater Systems
1340	17. Unknown
1341	
1342	39. [Op] + [RR] To the best of your knowledge, what is the current functional,
1343	informational, economic, and/or physical impact to other third parties that are not
1344	entities in a critical infrastructure sector? (DESIGN NOTE: Multi select)
1345	A. Functional impact
1346	1. Not applicable, there is no possibility of indirect functional impact to entities
1347	not in a critical infrastructure sector
1348	2. No impact at this time
1349	3. Low impact
1350	4. Moderate impact
1351	5. High impact
1352	6. Critical
1353	7. Unknown
1354	B. Informational impact

³⁷ **Physical Impact**: The resultant of an incident that has caused intentional or accidental damage to a physical system/facility/surrounding environment, that disrupts, incapacitates, or destroys reliable operations of critical infrastructure, including personnel therein.
1355	1.	Not applicable, there is no possibility of indirect informational impact to
1356		entities not in a critical infrastructure sector
1357	2.	No impact at this time
1358	3.	Low impact
1359	4.	Moderate impact
1360	5.	High impact
1361	6.	Critical
1362	7.	Unknown
1363	C. Eco	onomic impact
1364	1.	Not applicable, there is no possibility of indirect economic impact to entities
1365		not in a critical infrastructure sector
1366	2.	No impact at this time
1367	3.	Low impact
1368	4.	Moderate impact
1369	5.	High impact
1370	6.	Critical
1371	7.	Unknown
1372	D. Phy	vsical impact
1373	1.	Not applicable, there is no possibility of indirect physical impact to entities
1374		not in a critical infrastructure sector
1375	2.	No impact at this time
1376	3.	Low impact
1377	4.	Moderate impact
1378	5.	High impact
1379	6.	Critical
1380	7.	Unknown
1381	Impacts	Internal to the Entity
1382	Funct	tional Impacts to Entity
1383	40. [Op] +	[RR] To the best of your knowledge, what is the current functional impact ³⁸
1384	of this i	incident?
1385	A. No	impact to both non-critical and critical services (DISPLAY NOTE: Incident has no
1386	impa	net.)
1387	B. Nor	n-critical services:
1388	1.	No impact to non-critical services (DISPLAY NOTE: Incident has no impact to non-
1389	2	critical services.)
1390 1391	2.	LOW IMPACT TO NON-CRUTCAL SERVICES (DISPLAY NOTE: Incident has low impact on any business or on delivery to entity customers.)
1991		business of on denvery to entry customers.

³⁸ **Functional impact** is a measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), little or no impact may be experienced due to the incident (CISA National Incident Cyber Scoring System). <u>CISA National Cyber Incident Scoring System (NCISS) | CISA</u>

1392	3. Moderate impact to non-critical services (DISPLAY NOTE: Moderate impact to non-
1393	critical services. Some small level of impact to non-critical systems and services.)
1394	4. High impact to non-critical services (DISPLAY NOTE: Significant impact to non-
1395	critical services. A non-critical service or system has a significant impact.)
1396	5. Critical impact to non-critical services (DISPLAY NOTE: Denial of non-critical
1397	services. A non-critical system's access is denied, or system's functionality is destroyed.)
1398	6. Unknown
1399	C. Critical services:
1400	1. No impact to critical services (DISPLAY NOTE: Incident has no impact to critical
1401	services.)
1402	2. Low impact to critical services (DISPLAY NOTE: Incident has low impact on any
1403	industrial control systems (ICS) or on delivery of critical services to entity customers.)
1404	3. Moderate impact to critical services. ³⁹ (DISPLAY NOTE: Moderate impact to a critical
1405	system or service (e.g., email, active directory).)
1406	4. High impact to critical services (DISPLAY NOTE: A critical system has a significant
1407	impact (e.g., local administrative account compromise).)
1408	5. Critical impact to critical services (DISPLAY NOTE: Denial of critical services/loss of
1409	control. A critical system has been rendered unavailable.)
1410	$0. \mathbf{U}\mathbf{n}\mathbf{k}\mathbf{n}0\mathbf{w}\mathbf{n}$
1411	41. {Conditional} [Op] + [RR] (DESIGN NOTE: Only display question if response to "Functional
1412	impact" yields a "Low, Moderate, High, Critical, or Unknown" selection by the reporter for either non-
1413	critical or critical services). Please select (one) the most severe location any observed
1414	disruption in your entity's non-critical business or critical system networks from
1415	within your environment from this list:
1416	A. Business demilitarized zone (DMZ) (Activity was observed in the business
1417	network's demilitarized zone (DMZ))
1418	B. Business network (Activity was observed in the business or corporate network of
1419	the entity; these systems would include corporate user workstations, application
1420	servers, and other non-core management systems)
1421	C. Business network management (Activity was observed in business network
1422	management systems such as administrative user workstations, active directory
1423	servers, or other trust stores)
1424	D. Critical system DMZ (Activity was observed in the DMZ that exists between the
1425	business network and a critical system network. These systems may be internally
1425	facing services such as SharePoint sites financial systems or relay "jump" haves
1420	into more critical systems.)
1427	$\mathbf{F} = \mathbf{C} \cdot \mathbf{C} + \mathbf{C} + \mathbf{C} \cdot \mathbf{C} + $
1428	E. Critical system management (Activity was observed in high-level critical systems
1429	management such as human-machine interfaces in Industrial Control Systems)

³⁹ **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *Derived from "critical asset" page 135-136 and critically page 139 of <u>https://www.dhs.gov/publication/dhs-lexicon</u>*

1430	F. Critical systems (Activity was observed in the critical systems that operate critical
1431	processes.)
1432	G. Unknown
1433	H. Other [describe] (DESIGN NOTE: Open Text)
1434	Informational Impacts to Entity
1435	42. [Op] + [RR] To the best of your knowledge, what is the current informational
1436	impact ⁴⁰ of this incident?
1437	A. No impact
1438	B. Low impact
1439	C. Moderate impact
1440	D. High impact
1441	E. Critical impact (unrecoverable)
1442	F. Unknown
1443	Physical Impacts to Entity
1444	43. $[Op] + [RR]$ To the best of your knowledge, what is the current physical impact ⁴¹ of
1445	this incident?
1446	A. No physical impact to both property and systems
1447	B. Physical impacts to property:
1448	1. No impact to non-critical and critical property
1449	2. Low impact to property (DISPLAY NOTE: Damage to non-critical property)
1450	3. Moderate impact to property (DISPLAY NOTE: Damage to critical property. ⁴²)
1451	4. High impact to property (DISPLAY NOTE: Destruction of non-critical property)
1452	5. Critical impact to property (DISPLAY NOTE: Destruction of critical property)
1453	6. Unknown
1454	C. Physical impacts to systems:
1455	1. No impact to non-critical and critical systems
1456	2. Low impact to systems (DISPLAY NOTE: Damage to non-critical systems)
1457	3. Moderate impact to systems (DISPLAY NOTE: Damage to critical systems)
1458	4. High impact to systems (DISPLAY NOTE: Destruction of non-critical systems)
1459	5. Critical impact to systems (DISPLAY NOTE: Destruction of critical systems)
1460	6. Unknown

⁴⁰ **Informational Impact**: In addition to functional impact, incidents may also affect the confidentiality, integrity and availability of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. (CISA National Incident Cyber Scoring System). <u>CISA National Cyber Incident Scoring System (NCISS) | CISA</u>

⁴¹ **Physical Impact**: The resultant of an incident that has caused intentional or accidental damage to a physical system/facility/surrounding environment, that disrupts, incapacitates, or destroys reliable operations of critical infrastructure, including personnel therein.

⁴² **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *Derived from "critical asset" page 135-136 and critically page 139 of <u>https://www.dhs.gov/publication/dhs-lexicon</u>*

1461	Economic Impacts to Entity
1462	44. [Op] + [RR] To the best of your knowledge, what is the current economic impact ⁴³ of
1463	this incident? (DISPLAY NOTE: Estimate any costs or losses associated with the categories of economic
1464	impacts listed below. If you require further clarity on the meaning of these categories of economic impacts,
1465	see the CISA report: "Cost of Cyber Incident.".44)
1466	A. Incident investigation and forensic analysis
1467	1. Please provide estimates in U.S. dollars for each applicable category of
1468	economic impact (use a range from minimum to maximum where uncertain,
1469	or the same for both 1f known) (DESIGN NOTE: Repeated for each selected)
1470	B. Incident response and containment (including direct response, cleanup, and
1471	recovery costs)
1472	C. Lost revenue or productivity
1473	D. Theft, fraud, and direct financial losses (including any ransomware payments
1474	disbursed)
1475	E. Legal fees and regulatory fines
1476	F. Victim notification and protection services
1477	G. Other Losses (e.g., Loss of Intellectual Property)
1478	k.Incident Details
1478 1479	k.Incident Details Incident: Details by Stage
1478 1479 1480	k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in
1478 1479 1480 1481	k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer
1478 1479 1480 1481 1482 1483	k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage specific section of this report at any point if there is new information to report)
1478 1479 1480 1481 1482 1483	k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report.)
1478 1479 1480 1481 1482 1483 1483	 k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report.) I. Identification and Detection (I/D) Stage
1478 1479 1480 1481 1482 1483 1484 1484	 k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. I. Identification and Detection (I/D) Stage
1478 1479 1480 1481 1482 1483 1484 1485	 k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. I. Identification and Detection (I/D) Stage Incident Stage (I/D): Ransomware and Cyber Extortion
1478 1479 1480 1481 1482 1483 1484 1485 1486 1486	 k. Incident Details b. Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. I. Identification and Detection (I/D) Stage Disconter Stage (I/D): Ransomware and Cyber Extortion.
1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488	 k. Incident Details Incident: Details by Stage (DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r.2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. I. Identification and Detection (I/D) Stage Distign NOTE: Executes if incident is flagged as a Ransomware Incident in "Incident Type Determination" above as indicated in "red box" below:)
1478 1479 1480 1481 1482 1483 1484 1485 1485 1486 1487 1488	 k. Incident Details b. Details by Stage DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r.2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. b. Lanctification and Detection (I/D) Stage Discient Stage (I/D): Ransomware and Cyber Extortion. Chesign NOTE: Executes if incident is flagged as a Ransomware Incident in "Incident Type Determination" above as indicated in "red box" below:
1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488	 k. Incident Details b. Display NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r.2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. b. Identification and Detection (I/D) Stage DESIGN NOTE: Executes if incident is flagged as a Ransomware Incident in "Incident Type Determination" above as indicated in "red box" below: [RA] To the best of your knowledge, please select the categories involved in this [incident (DESIGN NOTE: With select, the drop down for more refined selections within each main (ategory, dropdown lists are in Appendix 3), (DESIGN NOTE: Wut have the drop pists "searchable" by
1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488	 k. Incident Details Display NoTE: Details by Stage (Display NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. b. Lacentification and Detection (L/D) Stage Display NOTE: Executes if incident is flagged as a Ransomware Incident in "Incident Type Determination" above as indicated in "red box" below: [Ra] To the best of your knowledge, please select the categories involved in this incident: (DISIN NOTE: Multi select, the drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (DESIGN NOTE: Multi select, due drop dworn for more refined selections within each mala regory, droptown lists are in Appendix 3.) (D
1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488	 b. Ancident Details b. Display NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. b. Checken Check
1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488	 k. Incident Details b. Display NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r.2, Computer Scorrity Incident Handling Guide). ⁴⁵ Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report. b. Checken Chec

⁴³ Economic Impact: Any costs or losses experienced due to an incident, including the general categories listed in this form in question #38A-G. These categories are more specifically defined in the CISA report: "Cost of Cyber Incident;" see Table 44 in Appendix C, <u>https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf</u>

⁴⁴ See Table 44 in Appendix C; https://www.cisa.gov/sites/default/files/2023-01/CISA-

OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

⁴⁵ https://csrc.nist.gov/pubs/sp/800/61/r2/final

1490	Initial Ransom Demand Details
1491	45. [RC] Please provide the following details about the ransom demand associated with
1492	this incident:
1493	A. [C-15] [Op] + [FISMA Req] Text of ransom demand(s) (DESIGN NOTE: Open text)
1494	B. [C-15] [Op] + [FISMA Req] Screenshot of ransom note(s) or copy of the email(s)
1495	C. [C-15] [Op] + [FISMA Req] Ransomware variant used (if known)
1496	D. [C-15] [Op] + [FISMA Req] Amount of ransom demand
1497	E. [C-15] [Op] + [FISMA Req] Currency type of ransom demand, including virtual
1498	currency
1499	F. [C-15] [Op] + [FISMA Req] Text of ransom payment instructions (if not already
1500	included in response to A, above) (DESIGN NOTE: Allow for a response to be "Same as
1501	response A", this is an open text otherwise.)
1502	G. [C-15] [Op] + [FISMA Req] Deadline given to pay ransom. Please provide the
1503	Date and Time (yyyy-mm-dd HH:MM - <utc offset="">) (DISPLAY NOTE: This could be</utc>
1504	a time in the future at time of report.)
1505	H. [C-15] [Op] + [FISMA Req] Description of any additional communications
1506	between the threat actors and either the impacted entity or a third party authorized
1507	to act on its behalf (e.g., phone conversations)
1508	I. [Op] + [FISMA Req] Does your organization have insurance that covers
1509	ransomware demand payments? (Yes/No)
1510	1. (DESIGN NOTE: If Yes) Please provide insurance company details
1511	a. Name
1512	b. Email address
1513	1. Unknown
1514	c. Website
1515	1. Unknown
1516	d. Physical address
1517	1. Street name and number
1518	2. Postal code
1519	3. City
1520	4. State
1521	5. Country
1522	e. Other contact information
1523	f. Insurance annual premium amount (DISPLAY NOTE: Primary carrier
1524	amounts if applicable, and if there is a separate cost for "ransom payments" only
1525	include that amount, otherwise total cost is acceptable.)
1526	1. Amount
1527	1. [] Select if primary carrier amount
1528	11. [] Kansom coverage only [] Total coverage (DESIGN
1229	2 Does the impacted entity plan on seeking or has it already sought coverage
1521	from its insurers for this incident? (Ves/No)
1721	

1532	Ransom Payment Details
1533	J. Ransom Payment Details
1534	1. [Op] + [FISMA Req] Was a ransom paid? (Yes/No)
1535	a. $\{Conditional\} + [OP] + [RR] (DESIGN NOTE: If Yes) Did your ransom$
1536	payment insurance cover the incident? (Yes/No) (DESIGN NOTE:
1537	Only ask if answered "Yes" to having ransomware insurance and planning to seek
1538	coverage.)
1539	2. {Conditional} [Op] + [FISMA Req] If ransom was paid, provide the
1540	following (DESIGN NOTE: Set Payment Count as 1.)
1541	(DESIGN NOTE: =======Ransomware Payment Details====================================
1542	a. [CUI] [Op] + [FISMA Req] Negotiation Details: Did you use a
1543	negotiation agent? (Yes/No), {Conditional} + [Op] + [FISMA
1544	Req] (DESIGN NOTE: If Yes) Provide
1545	1. [CUI]Negotiation agent point of contact
1546	i. [CUI]If person
1547	1. First
1548	2. Last
1549	3. Phone number(s)
1550	4. Email address(es)
1551	5. Position/title
1552	ii. If entity
1553	1. Name
1554	2. Email address
1555	i. Unknown
1556	3. Website
1557	i Unknown
1558	4 Physical address
1559	i Street name and number
1560	ii Postal code
1561	iii City
1562	iv State
1502	IV. State
1563	v. Country
1564	5. Other contact information
1566	person paying the ransom payment), the recipient (the person receiving the ransom payment), and how the
1567	transaction occurred can enable a more effective federal response to a ransom (or extortion) incident. CISA
1568	recognizes there may be multiple transactions over the course of the incident; this form will solicit the
1569	(potentially) unique details for each transaction separately.)
1570	b. [CUI] [Op] + [FISMA Req] Is the payer an individual or entity?
1571	(Select: Individual/entity) (DESIGN NOTE: Single select)
1572	1. [CUI]{Conditional} + [Op] + [FISMA Req] [Payer] (DESIGN
1573	NOTE: If Individual):

1574	i. First
1575	ii. Last
1576	iii. Phone number(s)
1577	iv. Email address(es)
1578	v. Position/title
1579	vi. Organization
1580	2. [CUI]{Conditional} + [Op] + [FISMA Req] [Payer] (DESIGN
1581	NOTE: If Entity):
1582	i. Entity name
1583	ii. [CUI] Point of contact
1584	1. First
1585	2. Last
1586	3. Phone number(s)
1587	4. Email address(es)
1588	5. Position/title
1589	iii. Entity email address
1590	1. Unknown
1591	iv. Website
1592	1. Unknown
1593	v. Physical address
1594	1. Street name and number
1595	2. Postal code
1596	3. City
1597	4. State
1598	5. Country
1599	vi. [CUI] Other contact information
1600	3. [CUI] [Op] + [FISMA Req] [Payer] Details of transaction per
1601	payment made to date: (DISPLAY NOTE: This is from the Payer's
1602	perspective. Additionally, the total ransom/extortion amount could be spread
1604	i Date and time payment was disbursed from the payer
1605	making the ransom payment to satisfy the ransom
1606	demand
1607	ii Currency type (traditional virtual/digital asset or other)
1608	1 Currency
1600	2 Other provide description (DESICN NOTE: Open text)
1610	iii Amount of navment (may be equal to or different from
1611	the actual demand)
1612	1 In virtual/digital asset
1612	2 In US dollar value at the time of the transaction
1012	

1614	iv. [CUI] For transactions that involved a bank or another
1615	type of financial institution (e.g., in facilitating the
1616	payment)
1617	1. Name of bank or financial institution
1618	2. Address of bank or financial institution
1619	i. Street name and number
1620	ii. Postal code
1621	iii. City
1622	iv. State
1623	v. Country
1624	3. Name(s) on the account
1625	4. Account number
1626	5. Routing number
1627	i. Origin
1628	v. [CUI] If virtual (e.g., crypto) currencies were used:
1629	1. Service used to
1630	i. Purchase the currency
1631	ii. Store the currency
1632	iii. Transmit the currency
1633	2. [CUI] Transaction ID (e.g., transaction hash), if
1634	known
1635	3. [CUI] Virtual (crypto) currency address(es)
1636	i. Payer addresses
1637	vi. Other method of paying the ransom / extortion demands
1638	1. [CUI] Describe the method
1639	vii. If the transaction occurred at a physical location, please
1640	provide
1641	1. Address of transaction
1642	i. Geographical point of interest (location)
1643	ii. Street name and number
1644	iii. Postal code
1645	iv. City
1646	v. State
1647	vi. Country
1648	2. Any other physical location characteristics describe
1649	here:
1650	c. [CUI] [Op] + [FISMA Req] To the best of your knowledge, is the
1651	recipient an individual, entity, or group?
1652	Select: []Individual []Entity []Group []Unknown (DESIGN NOTE:
1653	Skip "point of contact" info if "Unknown" selected) (DESIGN NOTE: Single
1004	select)

1655	1. [CUI] [Op] [FISMA Req if selected] [Recipient] (DESIGN
1656	NOTE: If Individual) Please provide the following information to
1657	the extent known:
1658	i. First
1659	ii. Middle
1660	iii. Last
1661	iv. Suffix
1662	v. Phone number(s)
1663	vi. Email address(es)
1664	vii. Social media information
1665	viii. Position/title
1666	2. [CUI] [Op] + [FISMA Req if selected] [Recipient] (DESIGN
1667	NOTE: If Entity/Group) Please provide the following information
1668	to the extent known:
1669	i. Name
1670	ii. [CUI] Point of contact at entity
1671	1. First
1672	2. Middle
1673	3. Last
1674	4. Suffix
1675	5. Phone number(s)
1676	6. Email address(es)
1677	7. Position/title
1678	iii. Entity email address
1679	iv. Entity social media information
1680	v. Entity website
1681	vi. Physical address
1682	1. Street name
1683	2. Street number
1684	3. Postal code
1685	4. City
1686	5. State
1687	6. Country
1688	vii. Any other contact information describe here:
1689	d. [CUI] [Op] + [FISMA Req if available] [Recipient] Details of
1690	transaction per payment: (DISPLAY NOTE: This is from the Recipient's
1691	perspective. Additionally, the total ransom/extortion amount could be spread among
1692	multiple payments and different methods.)
1004	 Date and time of ransom payment Currency type (traditional wirtual/digital or other)
1094	2. Currency type (traditional, virtual/digital, or other)
2601	1. Currency

 1697 3. Amount of ransom payment (may be equal to or different from the actual demand) 1699 In virtual/digital asset In US dollars 1700 In US dollars 1701 (CUI] For transaction(s) that involved a bank or another type of financial institution: Name of bank or financial institution Address of bank or financial institution 1704 Name of bank or financial institution 1705 Street name and number 1706 Postal code 1707 Street name and number 1708 Street name and number 1709 Country 1708 Street name and number 1710 Name(s) on the account 1711 V. Account number 1712 V. Routing number 1713 Destination 1714 Ustration (e.g., crypto) currencies were used Service used to 1. Purchase the currency Street name currency Street he currency Stre	1696	ii. Other, provide description (DESIGN NOTE: Open text)
1698 from the actual demand) 1699 i. In virtual/digital asset 1700 ii. In US dollars 1701 4. [CUI] For transaction(s) that involved a bank or another type 1702 of financial institution: 1703 i. Name of bank or financial institution 1704 ii. Address of bank or financial institution 1705 1. Street name and number 1706 2. Postal code 1707 3. City 1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1718 1. Purchase the currency 1719 1. Purchase the currency 1710 1. Purchase the currency 1711 1. Payee addresses 1712 1. Payee addresses 1714 1. Payee addresses 1715 1. Payee addresses 1720 1. Payee addresses 1721 1. Payee addresses <	1697	3. Amount of ransom payment (may be equal to or different
 i. In virtual/digital asset ii. In US dollars ii. In US dollars iii. In US dollars iii. Name of bank or financial institution iii. Address of bank or financial institution iii. Street name and number 2. Postal code 2. Postal code 3. City iii. Name(s) on the account iii. Country iii. Country iii. Service used to i. Service used to i. Service used to i. Purchase the currency iii. [CUI] Virtual (e.g., crypto) currencies were used iii. [CUI] Virtual (crypto) currency address(es) iiii. [CUI] Virtual (crypto) currency address(es) iii. [CUI] Virtual (crypto) currency address(es) iiii. [CUI] Virtual (crypto) currency address(es) iiiiin for apayment meta fifty associate pay at at the same ex	1698	from the actual demand)
 ii. In US dollars iii. In US dollars iii. In US dollars iii. CUI] For transaction(s) that involved a bank or another type of financial institution iii. Address of bank or financial institution iii. Street name and number iiii. Name(s) on the account iiii. Name(s) on the account iii. Street count number iiii. Street count number iiii. Street count on the account iiii. Street used to iiii. Street used to iii. Street used to iii. [CUI] Transaction ID (e.g., transaction hash), if known iii. [CUI] Virtual (crypto) currency address(es) iii. [CUI] Virtual (crypto) currency address(es) iii. [CUI] Virtual (crypto) (Design Note: If Ye, complete another session of "nament detals", associate payment installments iii. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Ye, complete another session of "nament detals", associate payment is to installment # 1. Previde an option to copy over from the first payment the information since it may be alt the same except for date/time.) iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	1699	i. In virtual/digital asset
1701 4. [CUI] For transaction(s) that involved a bank or another type of financial institution: 1702 of financial institution: 1703 i. Name of bank or financial institution 1704 ii. Address of bank or financial institution 1705 1. Street name and number 1706 2. Postal code 1707 3. City 1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Virtual (erg., installments 1720 1. Payee addresses 1721 V. Reve multiple payments made (e.g., installments 1722 I. Payee addresses 1723 I. Were multiple payment firstallments 1724 information information incident 1725 reg not	1700	ii. In US dollars
1702 of financial institution: 1703 i. Name of bank or financial institution 1704 ii. Address of bank or financial institution 1705 1. Street name and number 1706 2. Postal code 1707 3. City 1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1720 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1120 1. Payee addresses 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Y es/No) (Design Note: If Yes, complete another sesion of "payment details", associate payment # to installments + 1. Provide an option to copy over from the first payment the information sine it ma	1701	4. [CUI] For transaction(s) that involved a bank or another type
 i. Name of bank or financial institution ii. Address of bank or financial institution iii. Street name and number 2. Postal code 2. Postal code 3. City 3. City 3. Country 4. State 5. Country 5. Country 7. Routing number 7. Destination 7. Bervice used to 7. Purchase the currency 7. Store the currency 7. Transmit the currency 3. Transmit the currency utrency address(es) 7. Payce addresses 7. (CUI) Virtual (erg., installments 1. Payce addresses 7. Were multiple payments made (e.g., installments 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual]? (Yes/No) (Design Note: If Yes, complete another sestion of "payment details", associate payment # to installments 7. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual]? (Yes/No) (Design Note: If Yes, complete another sestion of "payment details", associate payment # to installments 7. Were multiple payment may be all the same except for date/time.) (DESIGN NOTE: MARCH) 7. Results of Ransom Incident 1. Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) a. (DESIGN NOTE: HYes) Did the keys work? 	1702	of financial institution:
 ii. Address of bank or financial institution iii. Street name and number iii. City iii. City iii. Name(s) on the account iii. I bestination i. Service used to i. Service used to i. Service used to i. Purchase the currency iii. [CUI] Virtual (c.g., transaction hash), if known iii. [CUI] Virtual (crypto) currency address(es) iii. [CUI] Virtual (crypto) currency address(es) iii. [CUI] Virtual (crypto) currency address(es) iiii. [CUI] Virtual (crypto) currency address(es) iiiiii. [CUI] Virtual (crypto) (besign Note: If Yes, complete another session of "payment details", associate payment # to installments, differing methods [some physical cash, some virtual])? (Yes/No) (besign Note: If Yes, complete another session of "payment details", associate payment # to installment # +1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: ADAGAAAA = End of Ransom Payment Details=ADAGAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	1703	i. Name of bank or financial institution
1705 1. Street name and number 1706 2. Postal code 1707 3. City 1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(cs) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	1704	ii. Address of bank or financial institution
1706 2. Postal code 1707 3. City 1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 110 1. Payee addresses 1722 1. Payee addresses 1723 1. Were multiple payment installments 1724 physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installments 1724 (DESIGN NOTE::AMARCH of Ransom Payment Details=*^AAAAAAA) 1725 Results of Ransom Incident 1726 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1724 physical cash, Nome Virtual])? 1725 of Ransom Incident 1726 <td< td=""><td>1705</td><td>1. Street name and number</td></td<>	1705	1. Street name and number
1707 3. City 1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be alt the same except for date/time.) (DESIGN NOTE:: MAACA_End of Ransom Payment Details=^^AAAAAAA) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1. Were you provided with decryption capabil	1706	2. Postal code
1708 4. State 1709 5. Country 1710 iii. Name(s) on the account 1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: MOTE: ^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	1707	3. City
17095. Country1710iii. Name(s) on the account1711iv. Account number1712v. Routing number17131. Destination17145. If virtual (e.g., crypto) currencies were used1715i. Service used to17161. Purchase the currency17172. Store the currency17183. Transmit the currency1719ii. [CUI] Transaction ID (e.g., transaction hash), if known17201. Payee addresses17211. Payee addresses17221. Payee addresses17231. Were multiple payments made (e.g., installments1724physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session1725of "payment details", associate payment # to installment # 1. Provide an option to copy over1726from the first payment the information since it may be all the same except for date(time.)1727(DESIGN NOTE: ^^^2 EEnd of Ransom Payment Details=^^^^^^^^1729L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident1730a. (DESIGN NOTE: If Yes) Did the keys work?	1708	4. State
 1710 1711 1712 1712 1713 1714 1714 1715 1715 1716 1. Purchase the currency 1717 1718 1718 1719 1719 1719 1720 1721 1721 1722 1721 1722 1723 1724 1725 1725 1726 1727 1727 1728 1728 1729 1720 1720 1720 1720 1721 1721 1722 1722 1723 1724 1725 1725 1725 1726 1726 1727 1728 183 193 193 193 193 193 100 193 194 194 194 194<	1709	5. Country
1711 iv. Account number 1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) 1725 of "payment flexiton" 1726 results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 a. (DESIGN NOTE: If Yes) Did the keys work? 1731 a. (DESIGN NOTE: If Yes) Did the keys work? </td <td>1710</td> <td>iii. Name(s) on the account</td>	1710	iii. Name(s) on the account
1712 v. Routing number 1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 1. Payee addresses 1723 1. Were multiple payments made (e.g., installments 1724 physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) 1725 (DESIGN NOTE:^^^^^^^	1711	iv. Account number
1713 1. Destination 1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 10. Payee addresses 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: ^^^^^^^^^^^^^^^^^^^ Cast of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 a. (DESIGN NOTE: If Yes) Did the keys work? 1731 actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1712	v. Routing number
1714 5. If virtual (e.g., crypto) currencies were used 1715 i. Service used to 1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: if yes) Color ransomware/cyber extortion incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 a. (DESIGN NOTE: If Yes) Did the keys work? 1731 actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1713	1. Destination
 i. Service used to Purchase the currency Purchase the currency Store the currency Transmit the currency Transmit the currency Transmit the currency [CUI] Transaction ID (e.g., transaction hash), if known [CUI] Virtual (crypto) currency address(es) [CUI] Virtual (crypto) currency address(es) Payee addresses Payee addresses K. [Op] + [FISMA Req] Identifying payment installments Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: ^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	1714	5. If virtual (e.g., crypto) currencies were used
1716 1. Purchase the currency 1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: ^^^^ CDESIGN NOTE: ^^^ CDESIGN NOTE: Method (e.g., keys) by the threat actor? (Yes/No) 1729 1. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 1. Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1715	i. Service used to
1717 2. Store the currency 1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: ^^^^^AOA^^AOA^=End of Ransom Payment Details=^^^^^AOA^AA^A) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 a. (DESIGN NOTE: If Yes) Did the keys work?	1716	1. Purchase the currency
1718 3. Transmit the currency 1719 ii. [CUI] Transaction ID (e.g., transaction hash), if known 1720 iii. [CUI] Virtual (crypto) currency address(es) 1721 1. Payee addresses 1722 K. [Op] + [FISMA Req] Identifying payment installments 1723 1. Were multiple payments made (e.g., installments, differing methods [some 1724 physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session 1725 of "payment details", associate payment # to installment # + 1. Provide an option to copy over 1726 from the first payment the information since it may be all the same except for date/time.) 1727 (DESIGN NOTE: ^^^^^^ Addressee End of Ransom Payment Details=^^^^^^^^ Addressee) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1717	2. Store the currency
 ii. [CUI] Transaction ID (e.g., transaction hash), if known iii. [CUI] Virtual (crypto) currency address(es) 1. Payee addresses K. [Op] + [FISMA Req] Identifying payment installments 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE: ^^^^ End of Ransom Payment Details=^^^^^^^) Results of Ransom Incident L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) a. (DESIGN NOTE: If Yes) Did the keys work? 	1718	3. Transmit the currency
 iii. [CUI] Virtual (crypto) currency address(es) Payee addresses Payee addresses K. [Op] + [FISMA Req] Identifying payment installments Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE:^^^^^=End of Ransom Payment Details=^^^^^^) Results of Ransom Incident I. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) a. (DESIGN NOTE: If Yes) Did the keys work? 	1719	ii. [CUI] Transaction ID (e.g., transaction hash), if known
 Payee addresses K. [Op] + [FISMA Req] Identifying payment installments Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE:^^^^^ = End of Ransom Payment Details=^^^^^^<) Results of Ransom Incident [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) a. (DESIGN NOTE: If Yes) Did the keys work? 	1720	iii. [CUI] Virtual (crypto) currency address(es)
 K. [Op] + [FISMA Req] Identifying payment installments Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE:^^^^=End of Ransom Payment Details=^^^^^^ Results of Ransom Incident [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) (DESIGN NOTE: If Yes) Did the keys work? 	1721	1. Payee addresses
1723 1. Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE:^^^^^=End of Ransom Payment Details=^^^^^^) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 1. Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1722	K. [Op] + [FISMA Req] Identifying payment installments
1724 physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE:^^^^^^=End of Ransom Payment Details=^^^^^^) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 1. Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1723	1. Were multiple payments made (e.g., installments, differing methods [some
1725 of "payment details", associate payment # to installment # + 1. Provide an option to copy over 1726 from the first payment the information since it may be all the same except for date/time.) 1727 (DESIGN NOTE:^^^^^=End of Ransom Payment Details=^^^^^^) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 1. Were you provided with decryption capabilities (e.g., keys) by the threat 1731 actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1724	physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session
1726 from the first payment the information since it may be all the same except for date/time.) 1727 (DESIGN NOTE:^^^^^=End of Ransom Payment Details=^^^^^) 1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 1. Were you provided with decryption capabilities (e.g., keys) by the threat 1731 actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1725	of "payment details", associate payment # to installment # + 1. Provide an option to copy over
1728 Results of Ransom Incident 1729 L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident 1730 1. Were you provided with decryption capabilities (e.g., keys) by the threat 1731 actor? (Yes/No) 1732 a. (DESIGN NOTE: If Yes) Did the keys work?	1726	from the first payment the information since it may be all the same except for date/time.) (DESIGN NOTE:^^^^^^=End of Ransom Payment Details=^^^^^^^)
1729L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident17301. Were you provided with decryption capabilities (e.g., keys) by the threat1731actor? (Yes/No)1732a. (DESIGN NOTE: If Yes) Did the keys work?	1728	Results of Ransom Incident
17301. Were you provided with decryption capabilities (e.g., keys) by the threat1731actor? (Yes/No)1732a. (DESIGN NOTE: If Yes) Did the keys work?	1720	$L_{\rm current}$ [CUI] [On] + [FISMA Real Results of ransomware/cyber extortion incident
1731actor? (Yes/No)1732a. (DESIGN NOTE: If Yes) Did the keys work?	1730	1. Were you provided with decryption canabilities (e.g., keys) by the threat
1732a. (DESIGN NOTE: If Yes) Did the keys work?	1731	actor? (Yes/No)
	1732	a. (DESIGN NOTE: If Yes) Did the keys work?
1733 b. What percentage of the files were recoverable (approximate)?	1733	b. What percentage of the files were recoverable (approximate)?
1734 2. To the best of your knowledge, was any data stolen? (Yes/No/Unsure)	1734	2. To the best of your knowledge, was any data stolen? (Yes/No/Unsure)
1735 (DESIGN NOTE: If Yes or Unsure):	1735	(DESIGN NOTE: If Yes or Unsure):

1736	a. [CUI] Describe the type of data stolen or suspected to have been
1737	stolen, to the best of your knowledge (DESIGN NOTE: Open text)
1738	b. [CUI] Did the threat actors leak any stolen data, to the best of your
1739	knowledge? (Yes/No) (DESIGN NOTE: If Yes) [describe]
1740	c. [CUI] Did the threat actors use any other pressure tactics, such as
1741	contacting third parties to inform them of the compromise?
1742	(Yes/No) (DESIGN NOTE: If Yes) [describe].
1743	3. [CUI] Describe any additional results of the ransom incident.
1744	M. [Op] + [FISMA Req] Did you experience follow-on attempts by threat actors to
1745	extort money or services? (Yes/No)
1746	{Conditional} [Op] + [FISMA Req] (DESIGN NOTE: If Yes) Did you pay the
1747	additional ransom or extortion demands? (Yes/No)
1748	(DESIGN NOTE: If Yes, repeat ===Ransomware Payment Details==)
1749	N. [Op] + [FISMA Req] Do you have any other information regarding the
1750	ransomware incident not previously provided (e.g., communications with the
1751	threat actors, transcripts, audio recordings, emails, chats)? (Yes/No)
1752	1. Describe (DESIGN NOTE: If Yes: Open text)
1753	Incident Stage (I/D): Tactics, Techniques and Procedures
1754	(TTPs) and Indicators of Compromise (IOCs) Observed
1755	46. [RA] Would you like to document the tactics, techniques, and procedures (TTPs) and
1756	related indicators of compromise(s) (IOCs) you observed by using our offline
1757	template and uploading the completed file, or would you prefer to proceed and enter
1758	the TTPs and IOCs directly in this online form?
1759	(DESIGN NOTE: select one) (DESIGN NOTE: If "Template" is selected, skip over following questions 47,
1760	48, 49, 50).
1/61	A. [] I'd like to use the offline template (DESIGN NOTE: If selected, proceed to Q47)
1762	B. [] I'd like to proceed with this report using the online form (DESIGN NOTE: If
1764	selected proceed to Q48)
1765	template to document your TTPs and IOCs, then will upload the file once complete
1766	Please proceed with the download of the template and instructions (below) and return
1767	to this point in the online form to unload your completed file
1769	A Download the TTP/IOC template/instructions here: DOWNI OAD
1760	TEMPI ATE/INSTRUCTIONS
1705	
1770	B. Upload the completed TTP/IOC file offline template here: UPLOAD
1771	TEMPLATE
1772	1. Select <u>here</u> to continue this report and return to upload your offline form
1773	later.
1774	

1775	Incident Stage (I/D): Tactics, Techniques and Procedures
1776	(TTPs) Observed
1777	48. {Conditional on Q46.B is selected} + [RA] You have indicated you want to
1778	document your TTPs and IOCs directly into this form. At this time, can you provide
1779	information regarding the TTPs the adversary leveraged as part of this incident?
1780	(Yes/No) (DESIGN NOTE: If No: DISPLAY NOTE: When, during your investigation, you discover
1781	knowledge about TTPs contributing to the incident, please return to this question and document them. If
1782	you have already documented and IOCs, you must also return to that section and provide the connections
1783	between the IOCs and TTPs documented that have factored into the incident.)
1784	49. ${Conditional}[RC]$ (DESIGN NOTE: Question applies only if "Yes" to TTPs to report selection of
1785	"Proceed directly in report" to documenting TTP/IOC in Q46.B) You have indicated you have
1786	TTP(s) to report and would like to document those TTP(s) and related IOC(s) directly
1787	in this online form. Therefore, please begin by selecting the type(s) of networks ⁴⁶ and
1788	systems the TTPs were observed within. (Select all that apply). []
1789	Enterprise/Traditional IT; [] Operational Technology/Industrial Control Systems; []
1790	Mobile Systems (DESIGN NOTE: Multi select)
1791	A. Are you familiar with the MITRE ATT&CK TTP framework? (Yes/No)
1792	
1793	B. Would you like to use CISA's internal tool to help you understand what TTPs you
1794	experienced? (Yes/No)
1795	1. (DESIGN NOTE: If Yes AND if No to "familiar with MITRE ATT&CK") Once you have
1796	completed using CISA's internal tool to help understand your TTPs, are you
1797	now able to use MITRE ATT&CK framework to identify your TTPs?
1798	(Yes/No)
1799	
1800	C. (DESIGN NOTE: If Yes to "familiar with the MITRE ATT&CK" {Conditional} [Op] +
1801	[FISMA Req] Select the appropriate MITRE ATT&CK tactics and/or
1802	technique(s) observed from the matrix associated with the network(s) you have
1803	selected
1804	1. One or more TTPs observed in this incident are not identified in MITRE
1805	ATT&CK, therefore we need to document those TTPs in a different method.
1806	[] Select if applicable (DESIGN NOTE: If selected allow for a combination of both
1807	MITRE ATT&CK TTP and alternate narrative method TTP identifications)

⁴⁶ Enterprise Networks: Networks and systems that consist of and/or support information for the following platforms: Windows, macOS, Linux, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network management devices (e.g., routers, switches, hubs, etc.), and Containers.

Industrial Control Networks: Operational Technology are programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (Operational technology - Glossary | CSRC (nist.gov))

Mobile Device Networks: Mobile devices/networks that have access to entity resources and network-based effects that can be used by adversaries. This includes supported devices for the following platforms: Android, iOS.

1809



1810 D. {Conditional} [Op] + [RR] (DESIGN NOTE: If "no" to familiar with MITRE ATT&CK) You 1811 have indicated you are unfamiliar using MITRE ATT&CK to identify TTPs 1812 observed used during this incident, or your entity observed TTP(s) not listed or 1813 that is currently unidentified in MITRE ATT&CK. Therefore, using the type of 1814 network(s) you have selected earlier, please select the TTP category that 1815 potentially matches the type of TTP you have observed: (DESIGN NOTE: Depending on 1816 which network selected earlier (Enterprise, ICS, Mobile) display the TTP category list (defined in "red 1817 1818 box" below) for each type of network and allow reporter to select one to many categories and allow a 1819 description narrative for each category chosen) (DESIGN NOTE: Provide "hover-over" descriptor of 1820 each category in each list to provide context/descriptor for the reporter.) 1821

Enternrise Networks	Mohile Networks	Industrial Control
	WIDDIE HEEWOIKS	Systems
Reconnaissance	Initial Access	Initial Access
Resource Development	Execution	Execution
Initial Access	Persistence	Persistence
Execution	Privilege Escalation	Privilege Escalation
Persistence	Defense Evasion	Evasion
Privilege Escalation	Credential Access	Discovery
Defense Evasion	Discovery	Lateral Movement
Credential Access	Lateral Movement	Collection
Discovery	Collection	Command and Control
Lateral Movement	Command and Control	Inhibit Response Function
Collection	Exfiltration	Impair Process Control
Commond and Control	Impact (physically to	Impact (physically to
Command and Control	data/systems)	data/systems)
Exfiltration		
Impact (physically to		
data/systems)		

1823 1824	i. Please provide a description and details of the TTPs observed in the category(ies) you have documented (DESIGN NOTE: Open text box)
1825	Incident Stage (I/D): Indicators of Compromise (IOCs) and
1826	associated Detection Methods Used
1827 1828 1829	(DISPLAY NOTE: In the next series of questions, you will be asked to provide Indicators of Compromise (IOCs) details and metadata observed and collected for each TTP selected.)
1830	50. [C-15] [RA] Do you have any Indicators of Compromise (IOCs) you can share with
1831	us? (Yes/No) (DISPLAY NOTE: You will be given an opportunity to associate reported IOC(s) with
1832	your entity's documented TTP(s) in a future step. (DESIGN NOTE: IF No: SKIP to Q52, the "Incident
1833	Stage (I/D): Malware Artifacts and Detection Logics/Analytics" section)
1834	(DESIGN NOTE: If Yes) There are two methods by which you can share IOCs with us.
1835	Option one is via a "copy/paste" of your IOC(s) into this form with opportunities to
1836	add additional IOC attributes once the system processes your "copy/paste". Option
1837	two is via providing the IOC(s) individually in a structured format wherein you
1838	provide attribute details and TTP mapping at the time of entry. (DISPLAY NOTE: Based
1839	on previous incident reporting and our experience, if there are 10 or fewer IOCs to report, the structured
1840	"individual build" approach may be the best option to document the IOCs.) Which method do you
1841	want to use to document your IOC(s)? [] "Copy/paste; [] "Individual build"
1842	
1843	1. [RC] (DISPLAY NOTE: To ensure we can ingest your data correctly you will need to provide
1844	your IOCs separated by a space, comma, semicolon, or new line.) Provide your IOC(s) via
1845	copy/paste here (DESIGN NOTE: Open text box)
1846	a. Upload via copy/paste method
1847	IOC Relation; Type; Context, Timeline [Start, Stop, Still ongoing (Y/N)]; IOC
1848	location observed
1849	1. Please validate and edit any errors to your IOC(s) here
1850	2. Based on the current IOC list reported, it is very helpful to
1851	CISA if you can provide additional context on the IOCs. The
1852	context which is particularly valuable to us is an explanation
1853	of whether the indicator is from the attacker, benign,
1854	unknown, the times seen, if the IOC is currently active in your
1855	environment, and the location the IOC was operating from
1856	within your network(s). It is preferred to have the attributes
1857	associated per individual IOC. At a minimum, the attributes
1858	can be applied to all IOCs of the same type. At what level are
1859	you able to provide us context on the IOC(s) you are sharing?
1860	[] Attributes per IOC entry [] Attributes per IOC type (Select
1861	(DESICN NOTE: Single select)
1967	3 Read on the IOC(s) added to your report places provide the
1002	5. Based on the IOC(s) added to your report, please provide the
1863	overall IOC attributes as necessary:

1864	i.	Were the	ese IOCs []Attacker, []Benign, []Unknown
1865		(Select a	ll that apply) (DESIGN NOTE: multi select)
1866	ii.	Please p	rovide the timeline of the IOC(s) collected
1867		1. First	known time IOC operational in your
1868		envii	ronment
1869		2. Is the	e IOC still active in your environment? (Y/N)
1870		(DESI	IGN NOTE: If No)
1871		i.	Time IOC ceased operation within your
1872			environment
1873	iii.	Please se	elect (one) the most severe location any of the
1874		IOCs we	ere operating from within your environment from
1875		this list:	
1876		i.	Business demilitarized zone (DMZ) (Activity
1877			was observed in the business network's
1878			demilitarized zone (DMZ))
1879		ii.	Business network (Activity was observed in the
1880			business or corporate network of the entity;
1881			these systems would include corporate user
1882			workstations, application servers, and other non-
1883			core management systems)
1884		iii.	Business network management (Activity was
1885			observed in business network management
1886			systems such as administrative user
1887			workstations, active directory servers, or other
1888			trust stores)
1889		iv.	Critical system ⁴⁷ DMZ (Activity was observed
1890			in the DMZ that exists between the business
1891			network and a critical system network. These
1892			systems may be internally facing services such
1893			as SharePoint sites, financial systems, or relay
1894			"jump" boxes into more critical systems.)
1895		v.	Critical system management (Activity was
1896			observed in high-level critical systems
1897			management such as human-machine interfaces
1898			in Industrial Control Systems)

⁴⁷ **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of <u>https://www.dhs.gov/publication/dhs-lexicon</u>*

1899		•	vi.	Critical systems (Activity was observed in the
1900				critical systems that operate critical processes.)
1901		v	'ii.	Unknown
1902		vi	ii.	Other [describe] (DESIGN NOTE: Open Text)
1903	4. Base	d o	n eac	h of the IOCs added to your report, please
1904	prov	ide	the in	ndividual IOC attributes as necessary
1905	i.	Wa	s the	IOC []Attacker, []Benign, []Unknown (Select
1906		one	e) (DE	SIGN NOTE: Single select)
1907	ii.	Plea	ase p	rovide the timeline of the IOC provided
1908		1.	First	known time IOC operational in your
1909			envi	ronment
1910		2.	Is th	e IOC still active in your environment? (Y/N)
1911			(DES	IGN NOTE: If No)
1912			i.	Time IOC ceased operation within your
1913				environment
1914	iii.	Plea	ase ii	ndicate any of these areas or locations in your
1915		org	aniza	ation's network(s) where you observed the IOC
1916		(sel	lect a	ll that apply)
1917		1.	Busi	ness demilitarized zone (Activity was observed
1918			in th	e business network's demilitarized zone [DMZ])
1919		2.	Busi	ness network (Activity was observed in the
1920			busi	ness or corporate network of the entity; these
1921			syste	ems would include corporate user workstations,
1922			appl	ication servers, and other non-core management
1923			syste	ems)
1924		3.	Busi	ness network management (Activity was
1925			obse	rved in business network management systems
1926			such	as administrative user workstations, active
1927			direc	ctory servers, or other trust stores)
1928		4.	Criti	cal system. ⁴⁸ DMZ (Activity was observed in the
1929			DMZ	Z that exists between the business network and a
1930			critic	cal system network. These systems may be
1931			inter	nally facing services such as SharePoint sites,
1932			finar	ncial systems, or relay "jump" boxes into more
1933			critic	cal systems.)

⁴⁸ **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. [derived from "critical asset" page 135-136 and critically page 139 of <u>https://www.dhs.gov/publication/dhs-lexicon</u>

1934	5. Critical system management (Activity was observed
1935	in high-level critical systems management such as
1936	human-machine interfaces in Industrial Control
1937	Systems)
1938	6. Critical systems (Activity was observed in the critical
1939	systems that operate critical processes.)
1940	7 Unknown
10/1	8 Other [describe] (DESIGN NOTE: Open Text)
10/2	b. Please associate the IOC(s) you provided with the appropriate
1942	TTD(a) way have already do any arted. If you have not not
1943	1 IP(S) you have already documented. If you have not yet
1944	documented any TTPs, please select [here] to omit this step for
1945	NOW. (DESIGN NOTE: if reporter selects "[here]" allow the IOC to TTP mapping
1946	process to be postponed and DISPLAY NOTE: When, during your investigation,
1947	you discover knowledge about 1 1 Ps contributing to the incident and have
1948	between the IOCs and TTPs documented that have factored into the incident)
1950	2. Individual build method (DESIGN NOTE: For Data marking: reporter needs the
1951	opportunity to label the following IOC information as proprietary at some point, e.g., through
1952	data markings/options to be marked in the CISA 2015 section.)
1953	a. Please select the TTP with which these IOCs are associated.
1954	(DESIGN NOTE: if reporter selects "[here]" allow the IOC to TTP mapping
1955	process to be postponed and DISPLAY NOTE: When, during your investigation,
1956	you discover knowledge about TTPs contributing to the incident and have
1957	documented them, please return to this question and provide the associations
1958	between the IOCs and TTPs documented that have factored into the incident.)
1959	(DESIGN NOTE: Select from TTP entered "pick-list" and allow reporter to
1961	(======DESIGN NOTE: This section is reneated for each type of IOC the
1962	reporter is providing ====)
1963	b. [Op] + [RR] What is the IOC's relation to the incident? (Attacker,
1964	Benign, Unknown) ((DESIGN NOTE: Select one)
1965	c. [C-15] [Op] + [RR] Select type of indicator of compromise (Select
1966	from list:):
1967	1. Autonomous System(s) (AS)
1968	2. Domain Name(s)
1969	3. Email Address(es)
1970	4. Email Message(s) (DESIGN NOTE: Allow option to upload Email
1971	Headers separate from Email Body.)
1972	5. IPv4 Address(es)
1973	6. IPv6 Address (es)
1974	7. Network Traffic
1975	8. URL
1976	9. File System Directory(ies)
1977	10. File Metadata
- · ·	

1978		11. Hash(es)
1979		12. Mutex(es)
1980		13. Software Metadata
1981		14. System Process(es)
1982		15. User Account(s)
1983		16. Windows Registry
1984		17. X.509 Certificate(s)
1985	d.	[C-15] + [RA] Please share any relevant context regarding these
1986		IOCs (DESIGN NOTE: Open text)
1987	e.	[Op] + [RR] Please enter your IOC timeline here
1988		1. First known time IOC operational in your environment
1989		2. Is the IOC still active in your environment? (Y/N) (DESIGN
1990		NOTE: If No)
1991		i. Time IOC ceased operation within your environment
1992	f.	[C-15] + [Op] + [RR] Please indicate any of these areas or
1993		locations in your organization's network(s) where you observed
1994		the IOC (select all that apply)
1995		
1996		i. Business demilitarized zone (Activity was observed in the
1997		business network's demilitarized zone [DMZ])
1998		ii. Business network (Activity was observed in the business
1999		or corporate network of the entity; these systems would
2000		include corporate user workstations, application servers,
2001		and other non-core management systems)
2002		iii. Business network management (Activity was observed in
2003		business network management systems such as
2004		administrative user workstations, active directory servers,
2005		or other trust stores)
2006		iv. Critical system ⁴⁹ DMZ (Activity was observed in the
2007		DMZ that exists between the business network and a
2008		critical system network. These systems may be internally
2009		facing services such as SharePoint sites, financial
2010		systems, or relay "jump" boxes into more critical
2011		systems.)

⁴⁹ **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of <u>https://www.dhs.gov/publication/dhs-lexicon</u>*

2012	v.	Critical system management (Activity was observed in
2013		high-level critical systems management such as human-
2014		machine interfaces in Industrial Control Systems)
2015	vi.	Critical systems (Activity was observed in the critical
2016		systems that operate critical processes.)
2017	vii.	Unknown
2018	viii.	Other [describe] (DESIGN NOTE: Open Text)
2019	Indicator of Comprom	ise (IOC) Individual Data Marking
2020	51. [RR except FISMA do not	show] Should the IOC(s) and associated detail you have
2021	provided in this section be	considered commercial, financial, and proprietary under
2022	the Cybersecurity Informa	tion Sharing Act of 2015? [Yes/No]
2023	Incident Stage (I/D): In	ndicators of Compromise (IOCs): Detection
2024	Methods	
2025	52. [Op] + [RR] MITRE's D3	FEND matrix categorizes countermeasures into multiple
2026	categories. Detection actio	ns are identified in the "Model" and "Detect" categories.
2027	Are you familiar with, and	/or would you like to use MITRE D3FEND matrix to
2028	document your detection n	nethods? (Yes/No)
2029	a. (DESIGN NOTE: If y	ves) Please select the detection methods you used to discover
2030	each observed ac	tivity IOC using the MITRE D3FEND matrix (DISPLAY
2031	NOTE: Please return	to this section at any point during the life cycle of this incident to
2032	document any addition	onal detection methods used to help resolve this incident)

						۵	knowledge o			M	,					
	A knowledge graph of cybersecurity countermeasures 0.14.0															
	ATT&CK Lookup				Search D3FEND's 620 Artifacts						laglata	Dagoing	ND Looku	Peatore		
	Asset	Network Mapping	Operational Activity Mapping	System Mapping	+	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	+	+	+	+
	Asset Vulnerability Enumeration	Logical Link Mapping	Access Modeling	Data Exchange Mapping		Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation	Administrative Network Activity	File Integrity Monitoring	Database Query String Analysis	Authentication Event Thresholding				
	Container Image Analysis	Active Logical Link	Operational Dependency Mapping	Service Dependency Mapping		Emulated File Analysis	Identifier Activity Analysis	Analysis Sender Reputation	Analysis Byte Sequence	Firmware Behavior Analysis	File Access Pattern Analysis	Authorization Event Thresholding				
	Configuration Inventory	Mapping Passive Logical	Operational Risk Assessment	System Dependency Mapping		File Content Analysis	Identifier Reputation Analysis	Analysis	Emulation Certificate Analysis	Firmware Embedded Monitoring	Indirect Branch Call Analysis	Credential Compromise Scope				
	Data Inventory	Link Mapping Network	Organization Mapping	System Vulnerability		File Content Rules	Domain Name Reputation Analysis		Active Certificate Analysis	Code Firmware	Process Code	Domain				
	Component Inventory	Traffic Policy Mapping				File Hashing	File Hash Reputation		Passive Certificate Analysis	Peripheral Firmware	Verification	Job Function				
	Network Node Inventory	Physical Link Mapping					IP Reputation		Client-server Payload	System	Modification Detection	Access Pattern Analysis				
	Software Inventory	Active Physical Link Mapping					URL Reputation		Connection Attempt	Operating System	Process Spawn Analysis	Local Account Monitoring Resource				
							URL Analysis		Analysis DNS Traffic Analysis	Endpoint Health	Process Lineage Analysis	Access Pattern Analysis				
									File Carving	Input	Script Execution Analysis	Session Duration Analysis				
									Inbound Session Volume Analysis	Analysis Memory Boundary	Shadow Stack Comparisons	User Data Transfer Analysis				
									IPC Traffic Analysis	Tracking Scheduled Job	System Call Analysis	User Geolocation Logon Pattern				
									Network Traffic Community Deviation	Analysis	File Creation Analysis	Analysis Web Session Activity				
									Per Host Download-	System		Analysis				
									Analysis	Analysis Service Binary						
									Anomaly Detection	Verification System						
2033			- 1						Relay Pattern Analysis	Analysis						
2034			b.	(DESI	GN NC	DTE: If	No) (D	ESIGN	NOTE: 1	Multi sel o dotor	lect)	achnicu	a tha	t n otor	stic 11	v fit
2035				1.	withir	our or	.gamz xistino	ation (5 "MI"	TRE D	a delet 3FENI) tacti	c" hut w	e illa	t poter st liste	nian d?	y m
2030					(Yes/]	No)	Albullg		INL D.	JI L I I		e outv	vus in	ot mote	a.	
2038					Ì. (D	ESIGN	NOTE	: If Yes):							
2039						1.	Whic	h tact	ic did y	our ac	tion fa	under	r?			
2040								a. M	lodel							
2041									1. As	set inv	entory	,				
2042									2. Ne	twork	mappi	ng				
2043									3. Op	eratior	nal acti	ivity ma	appin	g		
2044									4. Sys	stem n	nappin	g				
2045								b. D	etect							
2046									1. Fil	e analy	/sis					
2047									2. Ide	ntifier	analys	sis				
2048									3. Me	essage	analys	is				
2049	4. Network traffic analysis															

2050	5. Platform monitoring
2051	6. Process analysis
2052	7. User behavior analysis
2053	8. Description (DESIGN NOTE: Open text)
2054	II. (DESIGN NOTE: If No) If your organization is unable to use MITRE
2055	D3FEND, did not use any of the MITRE D3FEND detection
2056	methods, or is unsure which MITRE D3FEND detection method
2057	applies, select from the set of common detection methods below:
2058	1. Administrator
2059	2. Antivirus software
2060	3. Commercial and/or publicly available solution
2061	4. External source notification
2062	5. Human review
2063	6. Internally developed/proprietary solution
2064	7. Intrusion detection system (IDS)
2065	8. Log review
2066	9. User
2067	10. Unknown
2068	11. Other
2069	a. Please provide a description of the detection
2070	method(s). (DESIGN NOTE: Open text)
2071	Incident Stage (I/D): Malware Artifacts and Detection
2072	Logics/Analytics
2073	53. [C-15] [RA] Did you detect malicious software (malware) or scripts? (Yes/No)
2074	A. {Conditional} [Op] + [RR] (DESIGN NOTE: If Yes) Do you have any malware you
2075	can share with us? (Yes/No) (DESIGN NOTE: If Yes) Please upload here
2076	B. [C-15] {Conditional} [Op] + [RR] (DESIGN NOTE: If Yes) Please provide any
2077	additional detail or context regarding the malware you have shared with us
2078	(DESIGN NOTE: Open text)
2079	
2080	54. [Op] + [RR] Did you create any signatures or other detection analytics to identify
2081	and/or detect the threat activity you have reported? (Yes/No)
2082	{Conditional} [Op] + [RR] (DESIGN NOTE: If Yes)
2083	A. For each entry, please provide the following
2084	1. Description
2085	2. Pattern or rule
2086	3. Pattern or rule language or technology used (Yara, Snort, SIGMA, etc.)

2087	Incident Stage (I/D): Malware Artifacts and Detection
2088	Logics/Analytics: Data Classification Markings
2089	55. [CUI] [Op] + [RR] The default data marking for the malware artifacts and detection
2090	logic/analytics just reported is {insert default data marking here, default data marking
2091	is TBD} Would you like to change the default data marking? (Ves/No) (DISPLAY
2092	NOTE: The default marking with the lowest restriction available will be applied to fields not previously
2093	entered with a data marking label automatically to all submissions in the Malware Artifacts and Detection
2094	Logics/Analytics sub-section. Although you will be given an opportunity to change the markings for
2095	(Conditional) [On] + [PP] (DESIGN NOTE: 16 Ver) Which of these data markings best
2090	{Conditional} [Op] + [KK] (DESIGN NOTE: If Yes) which of these data markings best
2097	(DESIGN NOTE: See Appendix 1 for options)
2050	In sident Stage (I/D), Date Severage Used and Attribution
2099	Incident Stage (I/D): Data Sources Used and Attribution
2100	Data Sources Used
2101	56. [Op] + [RR] Were external data sources such as data from threat
2102	information/intelligence reporting used to discover or aid in discovering this incident?
2103	(Yes/No)
2104	[If Yes]Provide the following for each data source
2105	A. [Op] + [FISMA Req] Report title and number (if applicable)
2106	1. Name/description of data source (can include author, company providing the
2107	data source, or general description)
2108	2. Link to report/data source (if applicable and available to share)
2109	Attribution
2110	57. [RA] Have you attributed this incident to a threat actor? (Yes/No, This incident is
2111	currently an unattributed cyber intrusion/Maybe)
2112	{Conditional} [Op] (DESIGN NOTE: If Yes or Maybe) Provide the name of the "threat
2113	actor" and the source used to support this assessment below
2114	[] The attributed threat actor name and/or attribution source is classified (select if
2115	true)
2116 2117	DISPLAY NOTE: If you used a classified source to help in your attribution, do not complete the following. You will be contacted via a secure means to discuss further if necessary)
2118	A. Threat actor name (could be name of advanced persistent threat [APT] actor,
2119	ransomware group, etc.) (DESIGN NOTE: Open text)
2120	B. Was this attribution claim based on one of the data sources you previously
2121	provided? (DESIGN NOTE: Allow to select from list (one to many entries.))
2122	If not, please provide the attribution source(s) (DESIGN NOTE: One to many
2123	entries.)
2124	1. Name of attribution source(s) (DESIGN NOTE one to many entries.)
2125	2. URL/Web link to validate source material (DESIGN NOTE: One to many
2126	entries.) (DESIGN NOTE: Open text)
2127	3. Report title(s) and number(s) (if applicable) (DESIGN NOTE: One to many
2128	entries) (DESIGN NOTE: Open text)

2129 2130 2131 2132 2133 2134 2135 2136	 4. Other details (DESIGN NOTE: One to many entries.) (DESIGN NOTE: Open text) C. What is your level of confidence ⁵⁰ in your attribution (DESIGN NOTE: Select one) 1. Confirmed by other sources: confirmed by other independent sources; logical in itself; consistent with other information on the subject 2. Probably true: not confirmed; logical in itself; consistent with other information on the subject 3. Possibly true: not confirmed; reasonably logical in itself; agrees with some other information on the subject
2137	D. Provide any additional information you feel is relevant (DESIGN NOTE: Open text)
2138	(Conditional) [On] + [PP] (DESIGN NOTE, ISNO) This incident is currently an
2139	(Conditional) [Op] + [KK] (Design NOTE: If No) This includent is currently an unattributed cyber intrusion. Please provide any additional information you feel is
2140	relevant and will aid in attribution (DESIGN NOTE: Open text)
2111	Torovant and win and in attroation. (BESIGIVITOTE: Open text)
2142	m. Assistance
2143	Assistance from CISA
2144	58. [Op] + [RR] Are you interested in receiving incident response assistance from CISA
2145	to the extent available? (Yes/No)
2146	59. [Op] + [RR] Are you interested in additional collaboration or information sharing
2147	with CISA around this incident to the extent feasible? (Yes/No)
2148	Third Party Assistance
2149	60. [Op] + [RR] Are you utilizing an external third party to provide assistance with the
2150	reported incident? (Yes/No)
2151	A. (DESIGN NOTE: If Yes) Provide the name of third-party entity(ies) (DESIGN NOTE: Open
2152	text)
2153	Data Sharing and Logging Readiness
2154	61. [OP] + [RR] Are you willing to share the results of third-party analysis with CISA?
2155	(Yes/No) (DESIGN NOTE: Only Display if "Yes" to "third party" question prior.)
2156	62. [OP] + [RR] Are you willing to share data (such as logs or other technical artifacts)
2157	about this incident with CISA? (Yes/No)
2158	1. {Conditional} [Op] + [FISMA Req] [If Yes] Please select all categories of
2159	data (such as logs or other technical artifacts) you are willing to provide. If
2160	necessary, our request for logs and technical artifacts would encompass only
2161	information related to the incident (DESIGN NOTE: Multi select) (DISPLAY NOTE:
2162 2163	You are not being asked to share this data with CISA at this time/through this report. The purpose of this question is for CISA to understand the extent to which such data exists, and you
2164	are willing to share it with CISA for potential analysis.)
2165	a. Identity-based logs for the following

⁵⁰ <u>https://www.misp-project.org/taxonomies.html#_admiralty_scale</u> <u>https://www.threat-intelligence.eu/methodologies/</u>

2166		1. Identity and credential management
2167		2. Privileged identity and credential management
2168		3. Authentication and authorization
2169		4. User accounts and user account meta-data
2170	b.	Network
2171		1. Email filtering, spam, and phishing logs
2172		2. Network device infrastructure logs (for devices with multiple
2173		interfaces: interface MAC if correlated to the De-NAT IP
2174		address)
2175		3. Network device infrastructure logs (e.g., general logging,
2176		access, authorization, and accounting)
2177		4. Data loss prevention logs
2178		5. Network traffic (e.g., packet capture) artifacts
2179		6. Network traffic (e.g., Netflow, Enhanced Netflow, Zeek Logs,
2180		etc.) artifacts
2181	c.	Host:
2182		1. Operating systems (e.g., Windows infrastructure and
2183		operating systems, MacOS, BSD)
2184		2. PKI and other multifactor applications and infrastructure
2185		3. Antivirus and behavior-based malware protection
2186		4. Other host logs (e.g., operating system, database logs,
2187		application logs)
2188	d.	Vulnerability
2189		1. Vulnerability assessments
2190		2. Penetration test results
2191	e.	Mobile
2192		1. Mobile (phones and tablets) EMM (UEM) / MTD server logs
2193		2. Mobile (phones and tablets) EMM (UEM) / MTD agent logs
2194	f.	Containers:
2195		1. Container (e.g., supply chain, image, engine
2196		(MGT/orchestration, OS, cluster/pod events)
2197	g.	Cloud unique data not specified above
2198		1. Cloud environments (general events and general logging)
2199		2. System configuration and performance
2200		3. Virtualization systems
2201	h.	Mainframes
2202		1. Mainframe unique logging not covered above
2203	i.	Communications

2204	1. Any communications with the threat actors (either by the
2205	entity or another entity on behalf of the entity) (e.g., emails
2206	[with full headers and attachments], chats, etc.)
2207	2. Notes, transcripts, and audio recordings of any
2208	communications with threat actors
2209	j. Financial
2210	1. Any log files supporting financial records and accounts
2211	associated with the incident (DISPLAY NOTE: This is not intended to
2212	include actual financial account information, e.g., account numbers, etc.)
2213	k. Forensic images:
2214	1. Forensic images (e.g., full disk, system, volume etc.) relevant
2215	to the incident
2216	2. Memory images relevant to the incident
2217	1. Malicious code
2218	1. Malicious code and associated files related to the incident
2219	m. Exfiltrated data
2220	1. Data and metadata exfiltrated related to the incident (DISPLAY
2221	NOTE: This is not intended to include actual compromised data.)
2222	2. Evidence of data and metadata exfiltrated, related to the
2223	incident
2224	n. Reporting
2225	1. Forensic and other reporting related to or concerning the
2226	incident (internal or external party originated)
2227	
2228	n. Analysis (A) Stage ⁵¹
2229	63. [RA] Have you begun the analysis stage? (Yes/No/Unsure) (DISPLAY Note: The focus in
2230	this stage is on analyzing the incident in more detail, determining the root cause, and assessing the impact.)
2231	A. (DESIGN NOTE: If Yes) Please provide the date (yyyy-mm-dd) you began the analysis
2232	stage
2233	64. [FISMA Req] Has the suspicious activity been declared an incident? (Yes/No)
2234	(DISPLAY NOTE: This event and time is different from the first time of incident detection. An incident
2235	declaration is the point when your organization has officially analyzed the information and determined the
2230 2227	A (DESIGN NOTE: If Voc) Provide date and time (www.mm_dd HH·MM - <utc)< td=""></utc)<>
2237	offset>) the incident was declared
2230	onser juie mendent was declared

⁵¹ Analysis Stage - Stage of an incident life cycle that involves a process of examining [the systems] in terms of [but not limited to] their operation, configuration, and physical presence, in terms of "its constituent parts so as to reveal new meaning by investigation of the [system] elements to distinguish problems, situations, or anomalies for instructional solutions or other suitable interventions that optimize performance." Entering in the Analysis phase involves the transition from 'Something Happened' [Identification and Detection] to understanding 'What has Happened'. [derived from page28 of https://www.dhs.gov/publication/dhs-lexicon]

2239	Incident Stage (A): Impacted Users and Systems
2240	
2241	65. [RA] Please identify the impacted users (number of impacted privileged and/or
2242	standard information technology (IT) users) (DISPLAY NOTE: This is not necessarily all users,
2243	but those users impacted by activity during the incident.) (DESIGN NOTE: Multi select then quantity
2244	enterea.) A Privilagad/gystam/administrativa/garviga laval IT usar quantity impacted (DESIGN
2245	A. FINNEged/System/administrative/service-rever if user quantity impacted (DESIGN NOTE: Quantity)
2247	1. [Op] How are these users impacted (e.g., accounts locked, removed, other)?
2248	B. Standard IT user quantity impacted (DESIGN NOTE: Quantity)
2249	1. [Op] How are these users impacted (e.g., accounts locked, removed, other)?
2250	66. [C-15] [RA] With respect to information systems you own and/or operate that are
2251	impacted by or involved in this incident: (DESIGN NOTE: These set of questions repeat for
2252	every "instance" of Impacted Systems identified below.)
2253	A. [FISMA Req] + [FedRAMP] Please identify whether any impacted information
2254	system, network, and/or device supports any elements of the intelligence
2255	community or contains information that has been determined by the United States
2256	Government pursuant to an Executive Order or statute to require protection
2257	against unauthorized disclosure for reasons of national defense or foreign
2258	relations, or any restricted data, as defined in 42 U.S.C. 2014(y) (Yes/No).
2259	1. (DESIGN NOTE: If Yes) Please identify the relevant federal entity category
2260	(DESIGN NOTE: Multi select)
2261	a. Federal civilian executive branch (FCEB) - FISMA System
2262	(Yes/No)
2263	b. Intelligence community (Yes/No)
2264	c. Federal judicial branch (Yes/No)
2265	d. Federal legislative branch (Yes/No)
2266	e. DOD system, program, or platform (Yes/No)
2267	B. {Conditional} (DESIGN NOTE: Conditional to "Yes" selection to "A.1.a. Federal Civilian
2268	Executive Branch (FCEB) - FISMA System (Yes/No)". If Yes)
2269	1. [FISMA Req] Please provide the FISMA system name
2270	2. [FISMA Req] Please select the type of FISMA system
2271	a. General support system
2272	b. Major application
2273	c. Other
2274	1. Please provide the system type (DESIGN NOTE: Open text)
2275	3. [CUI] [FISMA Req] Contact information of the federal employee identified
2276	as the system owner
2277	a. Name
2278	1. First
2279	2. Last

2280	b. Phone number(s)
2281	1. Unclassified
2282	2. [Op]Classified
2283	c. Email address(es)
2284	1. Unclassified
2285	2. [Op]Classified
2286	d. Position or title
2287	C. [C-15] [RA] Identify and describe the function of each individual (or group of
2288	similar) affected network(s), device(s), and/or Information System(s), specifically
2289	with respect to the category, system type, services provided, name, location and
2290	government customer communities supported
2291	1. Category (Select all that apply) (DESIGN NOTE: Multi select)
2292	a. []Enterprise networks or systems ⁵² : Impacted [confirmed]
2293	[suspected] (Select one) (DESIGN NOTE: Single select)
2294	b. []Operational technology ⁵³ and industrial control systems:
2295	Impacted [confirmed] [suspected] (Select one) (DESIGN NOTE: Single
2296	select)
2297	c. []Mobile devices ⁵⁴ : Impacted [confirmed] [suspected] (Select
2298	one) (DESIGN NOTE: Single select)
2299	
2300	2. Systems type (DESIGN NOTE: Multi select then quantity entered)
2301	a. Endpoint devices (non-server devices)
2302	1. Authentication token or device
2303	i. Operating systems (OS) (DESIGN NOTE: 1.i.,ii.,iii and 2.,
2304	repeated for each option selected)
2305	i. OS name(s)
2306	ii. OS version number(s)
2307	iii. Number impacted of each OS version
2308	2. Desktop
2309	3. Laptop
2310	4. Media (e.g., backup tapes, disk media (e.g., CDs, DVDs),
2311	documents, flash drive or card, hard disk drive, media player,
2312	recorder)

⁵² Networks and systems that consist of and/or support information for the following platforms: Windows, macOS, Linux, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network management devices (e.g., routers, switches, hubs, etc.), and Containers.

⁵³ Operational Technology are programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (Operational technology - Glossary | CSRC (nist.gov)) ⁵⁴ Mobile devices that have access to entity resources and network-based effects that can be used by adversaries.

This includes supported devices for the following platforms: Android, iOS.

2313	5. Mobile phone or smartphone
2314	6. Peripheral (e.g., printer, copier, fax, identity smart card,
2315	payment card (such as a magstripe or EMV))
2316	7. Point of sale (POS) terminal
2317	8. Tablet
2318	9. Telephone
2319	10. Voice over Internet Protocol (VoIP) phone
2320	11. Other/unknown (DESIGN NOTE: Open text)
2321 b.	Server types
2322	1. Active Directory (AD) Components
2323	i. Operating systems (OS) (DESIGN NOTE: 1.i.,ii.,iii and 2.,
2324	repeated for each option selected)
2325	i. OS name(s)
2326	ii. OS version number(s)
2327	iii. Number impacted of each OS version
2328	2. Certificate Authority (CA)
2329	3. Domain Name System (DNS)
2330	4. Dynamic Host Configuration Protocol (DHCP)
2331	5. Email
2332	6. File
2333	7. File Transfer Protocol (FTP)
2334	8. Kerberos
2335	9. Lightweight Directory Access Protocol/Lightweight Directory
2336	Access Protocol over Secure Sockets Layer (LDAP/LDAP[S])
2337	10. Network Time Protocol (NTP)
2338	11. Print
2339	12. Remote log(s) (e.g., email, VPN, Syslog, R-Syslog, Syslog-
2340	NG)
2341	13. Remote Shell (RSH)
2342	14. Security Information and Event Management (SIEM)
2343	15. Secure Shell (SSH)
2344	16. TELNET
2345	17. Virtual Private Network (VPN)
2346	18. Web
2347	19. Voice over Internet Protocol (VoIP) Gateways
2348	20. Authentication, Authorization, and Accounting (AAA)
2349	Services (e.g., Radius, Terminal Access Controller Access-
2350	Control System [TACACS+])
2351	21. Operational (OT) and Open-Source Software (OSS) types
2352	(e.g., Apache HTTP Server)
2353	22. Other

2354	i. Please list the additional server type(s) (DESIGN NOTE:
2355	Open text)
2356	c. Network Devices
2357	1. Firewalls
2358	1. Operating systems (OS) (1.i, ii and iii. repeated for
2359	each selected)
2360	i. OS name(s)
2361	ii. OS version number(s)
2362	iii. Number impacted of each OS version
2363	2. Intrusion Detection System (IDS)
2364	3. Intrusion Protection System (IPS)
2365	4. Hub
2366	5. Load Balancers
2367	6. Proxies
2368	7. Routers
2369	8. Switches
2370	9. Other
2371	i. Please list the additional network device type(s) (DESIGN
2372	NOTE: Open text)
2373	d. Identity providers (IdP)
2374	1. Active Directory
2375	2. Active Directory Federation Services (ADFS)
2376	3. Amazon
2377	4. Azure Active Directory
2378	5. Facebook
2379	6. Google Workspace
2380	7. Lightweight Directory Access Protocol (LDAP)
2381	8. Login.gov
2382	9. Ping Federate
2383	10. OpenID Connect
2384	i. Provide the name of the provider(s) (DESIGN NOTE: Open
2385	text)
2386	11. Okta
2387	12. Security Assertion Markup Language (SAML)
2388	i. Provide the name of the provider(s) (DESIGN NOTE: Open
2389	text)
2390	13. Other identity providers
2391	i. Please provide the name of the identity provider(s)
2392	(DESIGN NOTE: Open text)
2393	3. Name of system(s) (DISPLAY NOTE: Provide name of system to add fidelity to the system
2394 2395	(or group of systems) that is entered in this instance (e.g., clarifying names of servers.)) (DESIGN NOTE: Open text)

2396	4. Name of system(s) services provided (e.g., active directory, email, web,
2397	boundary firewall, key personnel mobile device) (DESIGN NOTE: Open text)
2398	5. Physical location(s) of system or group of systems
2399	a. [] Select if same as impacted facility address entered earlier
2400	b. If not the same address as impacted facility, then please provide
2401	address of impacted system(s)
2402	1. Street name and number
2403	2. City
2404	3. State
2405	4. Postal code
2406	5. Country
2407	6. Is the impact or involvement of the system (or group of systems) identified []
2408	confirmed or [] suspected at the time of report? (DESIGN NOTE: Select one.)
2409	
2410	D. $[Op] + [RR]$ Is the system identified as part of the High Value Asset (HVA) ⁵⁵
2411	Program (Yes/No)
2412	E. [Op] + [RR] Is the impacted system designated as a National Security System. ⁵⁶
2413	(Yes/No)
2414	F. {Conditional}(DESIGN NOTE: Conditional to "Yes" selection to D. High Value Asset (HVA)
2415	Program (Yes/No).)
2416	1. What is the HVA Identification Number?
2417	2. For each HVA listed, what services does it provide?
2418	a. For each service, what communities does it support? (DESIGN NOTE:
2419	Open text)
2420	3. Does this HVA have connections to other HVAs? (Yes/No)
2421	a. (DESIGN NOTE: If Yes) Are these connections internal to the agency,
2422	external to the agency, or both? (Internal/External/Both)
2423	b. (DESIGN NOTE: If Yes) Do you know what the other HVAs are?
2424	(Yes/No)
2425	1. (DESIGN NOTE: If Yes) Please list the other $HVA(s)$.
2426	i. For each HVA listed, what services does it provide?
2427	(DESIGN NOTE: Open text)
2428	1. For each service, what communities does it support?
2429	(DESIGN NOTE: Open text) 2 Do you have contact information for the other $HVA(s)^2$
2430	(V_{as}/N_{a})
2431	(1 C) (1 C)
2432	1. [UUI] (DESIGN NOTE: If Yes)
2433	1. Name

 $^{^{55}\} https://www.cisa.gov/resources-tools/programs/high-value-asset-program-management-office$

⁵⁶ NSS is defined in law here: <u>40 USC 11103: Applicability to national security systems (house.gov)</u> https://uscode.house.gov/view.xhtml?req=(title:40%20section:11103%20edition:prelim)%20OR%20(granuleid:US C-prelim-title40-section11103)&f=treesort&num=0&edition=prelim

2434	i. First						
2435	ii. Last						
2436	2. Phone number(s)						
2437	i. Unclassified						
2438	ii. [Op]Classified						
2439	3. Email address(es)						
2440	i. Unclassified						
2441	ii. [Op]Classified						
2442	4. Position or title						
2443	5. Time zone						
2444	Incident Stage (A): Initial Access "Patient Zero" Detai	ls					
2445							
2446	67. $Conditional[Op] + [RR]$ (DESIGN NOTE: Executes if reporter has identified one	Initial Access					
2447	or more TTPs observed above in the "Initial Access" category in any of the MITRE	10 techniques					
2448	ATT&CK TTP matrices (example in "red box" to the right), this list is a "Dynamically	Content Injection					
2449	created" list at time of question determined by which MITRE ATT&CK "Initial Access"						
2450	TTPs were selected.) You have observed and identified an "initial access"						
2451	TTP ³⁷ in this incident. Have you identified the initially affected	Facing Application					
2452	endpoint, device, account, and/or application commonly referred to as	External Remote Services					
2453	"patient zero"? (Yes/No) (DESIGN NOTE: If Yes, go to Q 69.)	Hardware Additions					
2454	68. {Conditional}[Op] + [RR] (DESIGN NOTE: Trigger this question if no MITRE						
2455	ATT&CK TTPs were entered to identify any Initial Access TTPs and the narrative						
2456	response has been parsed into discrete TTPs to create a list.) Have you identified any	Removable Media					
2457	initial access TTPs that you have attributed as the initial entry into your	Supply Chain Compromise (3)					
2458	networks, commonly referred to as "patient zero"? (Yes /No) (DESIGN	Trusted Relationship					
2459	NOTE: If Yes, go to Q 69.)	, Valid					
2460	69. {Conditional}[Op] + [RR] > [Triggered only if "Yes" from either Q67	Accounts (4)					
2461	or Q68] Please select from your reported initial access observed activity: 7	TP(s) and					
2462	provide the technique used to gain the initial access to patient zero.						
2463	A. (DESIGN NOTE: If Yes) Was the "patient zero" already entered with the re	st of the					
2464	impacted systems? (Yes/No)						
2465	1. (DESIGN NOTE: If Yes) Please select from your list of impacted syste	ms the					
2466	system(s) you believe to be "patient zero." (DESIGN NOTE: Allow to s	elect from					
2467	previously entered impacted system (from question highlighted in "red box" below) list of "table					

⁵⁷ Tactics, Techniques and Procedures (TTP)

2468	responses" and if not already entered, then allow for a similar table entry.				
	C-15][RA] With respect to information systems you own and/or operate that are				
	impacted by or involved in this incident: (DESIGN NOTE: These set of questions repeat for				
	A. [C- <u>15][</u> RA] Identify and describe the function of each individual (or group of				
	similar) affected network(s), device(s), and/or Information System(s),				
	location and government customer communities supported:				
	1. Category:				
	a. Enterprise Networks or Systems ⁴⁷ : Impacted [confirmed, suspected]				
	b. Operational Technology ⁴⁸ and Industrial Control Systems:				
	Impacted [confirmed, suspected]				
	c. Mobile Devices*?: Impacted [confirmed, suspected]				
	2. Systems Type (DESIGN NOTE: Multi select then quantity entered) (DESIGN NOTE:				
	Modify drop lists as accordingly per system category above, [e.g., if mobile device is selected, don't include options for "desktops" as an Endpoint device])				
	a. Endpoint Devices (non-Server devices)				
	i. Operating Systems (OS) (DESIGN NOTE: 1.i.,ii, iii and 2.,				
	repeated for each option selected)				
	ii. OS version number(s)				
	iii. Number impacted of each OS <u>version</u>				
2460	2. Desktop $-3 - Lantop$				
2409	B. [C-15] (DESIGN NOTE: If "No" or the system was not found in preexisting list then:) If the				
2471	system is not vet entered, please enter "patient zero" details now.				
2472	1. Select the initial access system category and type (DESIGN NOTE: Follow same				
2473	format as in previous Impacted System entries. Pull from the list already identified in question				
2474	"Please Identify Impacted System". If already entered, allow reporter to select the system as				
2475	"Patient Zero", otherwise allow reporter to enter in Patient Zero system details in same format.)				
2476	C. When was the date/time of initial access in this incident?				
2477	1. Date and Time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>				
2478					
2479	Incident Stage (A): Detailed Informational Impacts				
2480	70. {Conditional}[FISMA Req + FedRAMP reporting only] (DESIGN NOTE: Display only if				
2481	"Classified data 'spillage' to unapproved networks" is selected in Incident Result. Reference "red box"				
2482	below:)				
	. [RA] This incident has led to or resulted in: (DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)				
	→ A. Classified data "spillage" to unapproved networks				
	B Compromised system(s)				
	C Destruction of data or systems (not due to Ransomware)				
2483					
2484	You indicated earlier that the incident resulted in spillage of classified information,				
2485	please provide more details below (DISPLAY NOTE: DISCLAIMER Do NOT provide any				
2486	classified information in the following responses)				
2487	A. what classification guide or source material was used to validate that the				
2488	information spilled was classified?				
2489	B. What was the root cause of the spillage? (DESIGN NOTE: Open text)				

2490	C. [CUI]Has an appeal or challenge been issued on the spillage of classified					
2491	information? (Yes/No)					
2492	1. On what date?					
2493	2. [CUI]To whom was the appeal or challenge issued?					
2494	3. Has the appeal been completed? (Yes/No)					
2495	4. Was this appeal accepted or denied? (Accepted/Denied)					
2496	a. If so, on what date was the appeal accepted or denied?					
2497						
2498	(DESIGN NOTE: Execute this question if any impact is selected from the earlier Informational Impacts to					
2499	Entity was selected (e.g., do NOT show if "No Impact" or "Unknown" were selected).)					
	[Op] + [RR] To the best of your knowledge, what is the current informational)					
	A. No impact					
	B. Low impact					
	C. Moderate impact					
	D. High impact					
2500	F. Unknown					
2501	71. {Conditional}[RC] Earlier in the form, you selected an informational impact ⁵⁸ to					
2502	your entity of (DESIGN NOTE: Place selected choice of Informational Impact question here, e.g., "High					
2503	Impact"). We would like more details on your information impacts; can you please					
2504	provide more details on any "suspected, but not confirmed" and/or "confirmed"					
2505	known informational impact(s) from the incident?					
2506						
2507	A. Please provide details on the "suspected" and/or "confirmed" informational					
2508	impact(s) from this incident: (DESIGN NOTE: (Multi select)					
2509	i. [] Suspected, but not yet confirmed					
2510	1. Which of these information types do you suspect was impacted?					
2511	(DESIGN NOTE: Multi select)					
2512	a. Classified material (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option					
2513	selected) (DESIGN NOTE: if these follow-on questions are same per info type					
2514	How was the suspected information impact discovered?					
2515	(Select all that apply)					
2510	(Select all that apply)					
2517	1. Some evidence of access but unclear evidence of					
2518	exiliarion					
2519	11. I hreat actor has provided inconclusive evidence of					
2520	information impact (e.g., pictures of file directories)					

⁵⁸ **Informational Impact**: In addition to functional impact, incidents may also affect the confidentiality, integrity and availability of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. (CISA National Incident Cyber Scoring System). <u>CISA National Cyber Incident Scoring System (NCISS) | CISA</u>

2521	iii. Other inconclusive evidence of threat actor access/use of
2522	the information (please describe) (DESIGN NOTE: Open text if
2523	selected)
2524	iv. We were informed by an independent third party
2525	2. Was the system where the information was located a critical
2526	system ⁵⁹ ? (Yes/No)
2527	b. Communications (e.g., emails, instant messages)
2528	c. Administrative credentials
2529	d. User or other non-administrative credentials
2530	e. Financial
2531	f. Dissemination controlled
2532	1. Legal
2533	2. Proprietary
2534	3. Other personal information
2535	g. Defense information (as the information relates to unclassified
2536	cyber threat information/indicators (CTI), export controlled,
2537	operational security (OPSEC) and/or information)
2538	1. Unclassified CTI
2539	2. Export controlled information
2540	3. OPSEC information
2541	
2542	ii. [] Confirmed
2543	1. (DESIGN NOTE: If Yes) What type of information impact? (DESIGN NOTE:
2544	Select Privacy Data Breach and/or Other Data Compromise and/or Credential
2545	Compromise) (DESIGN NOTE: Multi select)
2546	a. [] Privacy data breach (DESIGN NOTE: If Privacy data breach, then ask
2547	following) (DESIGN NOTE: Multi select)
2548	1. What type of information was impacted? (DESIGN NOTE: Multi
2549	select)
2550	1. Financial (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option
2551	selected)
2552	1. How was the information loss identified? (Select all
2553	that apply)
2554	1. The information was seen outside the authorized
2555	system (e.g., darkweb, leaksite, etc.) (DESIGN
2556	NOTE: Flagged as exploited)

⁵⁹ **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of <u>https://www.dhs.gov/publication/dhs-lexicon</u>*

2557			ii. Tl	he information was seen being exfiltrated from
2558			th	e authorized system and/or network (DESIGN
2559			NO	DTE: Flagged as loss)
2560		i	ii. W	e were informed by an independent third
2561			pa	arty (DESIGN NOTE: Flagged as loss)
2562		i	iv. O	ther evidence of threat actor access/use of the
2563			in	formation (please describe) (Design Note: Open
2564			Те	ext if selected)
2565		2.	Was the	e system where the information was located a
2566			critical	system? (Yes/No)
2567	ii.	Dis	seminat	ion Controlled
2568		1.	Legal	
2569		2.	Proprie	tary
2570		3.	Other p	ersonal information
2571				
2572 b.	[] Oth	er dat	ta comp	romise (DESIGN NOTE: If Other data compromise,
2573	then ask	the fo	llowing)	
2574	1. W	hat ty	ype of ir	nformation was impacted? (DESIGN NOTE: Multi
2575	sel	lect)		
2576	iii.	Cor	nmunic	ations (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for
2577		each	option se	lected)
2578		1.	How w	vas the information loss identified
2579			i. Tl	he information was seen outside the authorized
2580			sy	stem. (e.g., darkweb, leaksite, etc.)
2581			ii. Tl	he information was seen being exfiltrated from
2582			th	e authorized system and/or network
2583		i	ii. W	ve were informed by and independent third
2584			pa	arty
2585		i	iv. O	ther evidence of threat actor access/use of the
2586			in	formation (please describe)
2587		2.	Was the	e system where this information was located a
2588			critical	system? (Yes/No)
2589	i.	Diss	seminati	ion controlled
2590		i.	Propr	ietary
2591	ii.	Clas	sified	
2592	iii.	Defe	ense info	ormation (as the information relates to
2593		uncl	assified	cyber threat information/indicators (CTI),
2594		expo	ort contr	olled, OPSEC and/or information)
2595		i.	CTI	
2596		ii.	Expo	rt controlled information
2597		iii.	OPSE	C information

2598							
2599	c. [] Credential compromise (DESIGN NOTE: If credential compromise, then						
2600	ask the following)						
2601	a. What types of credentials were compromised? (DESIGN						
2602	NOTE: Multi select)						
2603	1. User or other non-administrative credentials						
2604	(DESIGN NOTE: 1.i.,ii.,iii.,iv and 2., repeated for each option selected)						
2605	1. How did you or others identify the compromise of						
2607	the credentials? (Select all that apply)						
2608	A. The information was seen outside the						
2609	authorized system (e.g., darkweb, leaksite,						
2610	etc.)						
2611	B. The information was seen being						
2612	exfiltrated from the authorized system						
2613	and/or network						
2614	C. We were informed by an						
2615	independent third party						
2616	D. Other evidence of threat actor						
2617	access/use of the information (please						
2618	describe) (DESIGN NOTE: Open Text if selected)						
2619	2. Was the system where this information was						
2620	located a critical system? (Yes/No)						
2621	ii. Administrative credentials						
2622	1. How was the compromise of the credentials						
2623	identified? (DESIGN NOTE: Select all that apply)						
2624	A. The information was seen outside the						
2625	authorized system. (e.g., darkweb,						
2626	leaksite, etc.)						
2627	B. The information was seen being						
2628	exfiltrated from the authorized system						
2629	and/or network (DESIGN NOTE: Flagged as loss)						
2630	C. We were informed by an						
2631	independent third party (DESIGN NOTE:						
2632	Flagged as loss)						
2633	D. Other evidence of threat actor						
2634	access/use of the information (please						
2635	describe) (DESIGN NOTE: Open Text if selected)						
2636	2. Was this credential on or did it have access to a						
2637	critical system? (Yes/No)						
2638							
2639	Incident Stage (A): Breach Details						
---	---	--	--	--	--		
2640 2641 (DESIGN NOTE: Encenter if incident in florend on a Breach Incident in "Breach Service"							
2641	(DESIGN NOTE: Executes if incluent is flagged as a Breach incluent in "Breach Severity Assessment" earlier as indicated in response to questions flagged in "red box" below:)						
	Breach ²⁵ Severity Impacts						
	unauthorized access to personally identifiable information? (Yes/No) (DESIGN NOTE: If						
	y'es, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access due" and "accessed by" only if "Yes".)						
	A. Was the access due to (select all that apply):1. Loss of control						
	2. Compromise						
	4. Unauthorized acquisition						
	B. Was the information accessed by (select all that apply):						
	2. An authorized user who accessed the record(s) for an other-than-authorized						
2643	purpose						
	{Conditional}[Op] + [FISMA Req] (DESIGN NOTE: Do not ask this question if the "Confirmed Unauthorized Access" question yields a positive selection response. Only ask if previous response to						
	"confirmed" = "No") At this time, has the incident resulted in any potential unauthorized						
	Breach Incident and include Information (1 ES 140) (DESIGN NOTE: 11 Fe, hag as Breach Incident and includent Stage (A): Breach Details. Show follow-on short questions "access due" and "accessed by" only if Was")						
	A. Was the potential unauthorized access due to: (select all that apply)						
	1. Loss of control 2. Compromise						
	3. Unauthorized disclosure						
	B. Was the information potentially accessed by: (select all that apply)						
	 A person other than an authorized user An authorized user who accessed the information for an other-than- 						
2644	authorized purpose						
2645	72. {Conditional}[Op] + [FISMA Req] Earlier in this form, you provided the following						
2646	description of this incident: (DESIGN NOTE: Pull forward the information entered by reporter						
2647	earlier as flagged in the "red box" below:)						
	[RA] Provide a high-level summary of the incident. (DESIGN NOTE: Open Text) (DISPLAY						
	NOTE: Requests for more details will occur later in this report. Please provide a short "Executive						
	Summary" of the incident with a narrative of the incident detection. Consider including a description of						
	any unauthorized access (including whether the includint involved an unattributed cyber intrusion); identification of any informational impacts or information compromise; any network location where						
	activity was observed; and a high-level description of the impacted system(s) (e.g., "email servers, a						
	network firewall, and a web server").)						
2648							
2649	You have also previously indicated there was actual or potential unauthorized access						
2650	to personally identifiable information (PII). Please add any available additional						
2651	context on the PII that was impacted. However, DO NOT include samples of actual						
2652	PII in this response.						
2653	73. [FISMA Req] Did this incident involve a cyber- or non-cyber-related breach of PII?						
2654	(DESIGN NOTE: Single-select)						
2655	A. Cyber-related						
2656	B. Non-cyber related (e.g., personnel information with PII found in a public						
2657	dumpster)						
2658	C. Both						

2659	74. [FISMA Req] If you have any additional details regarding what has been observed or
2660	identified with respect to the PII breach, please describe that here. However, DO
2661	NOT include samples of actual PII in this response. (DESIGN NOTE: Open text)
2662	Impacted Individuals
2663	75. [FISMA Req] How many individuals' PII was impacted. ⁶⁰ ?
2664	76. [FISMA Req] Were affected individuals notified? (Yes/No/Pending)
2665	A. (DESIGN NOTE: If Yes or Pending) How were (or will the) individuals (be) notified?
2666	(Select all applicable)
2667	1. Email
2668	a. How many individuals were (or will be) notified using this
2669	method?
2670	2. Short message service (SMS)
2671	a. How many individuals were (or will be) notified using this
2672	method?
2673	3. Verbal
2674	a. How many individuals were (or will be) notified using this
2675	method?
2676	4. Parcel
2677	a. How many individuals were (or will be) notified using this
2678	method?
2679	5. Other (Please list the method that was or will be used)
2680	a. How many individuals were notified using this method?
2681	77. [CUI] [FISMA Req] Were mitigation services in the form of monitoring, insurances
2682	and/or counseling provided or offered to affected individuals? (Yes/No)
2683	A. (DESIGN NOTE: If Yes) Which mitigation services have you made available to
2684	impacted individuals? (Please select all that apply):
2685	1. Identity monitoring
2686	2. Credit monitoring
2687	3. Identity theft insurance
2688	4. Full-service identity counseling and remediation services
2689	5. [CUI] Other (describe)
2690	PII Accessed and/or Impacted
2691	78. [FISMA Req] For each type of PII, provide how many records instances of a PII
2692	category or type were accessed, potentially accessed, or otherwise impacted?
2693	(DISPLAY NOTE: Use approximate counts if final counts are not available) (DESIGN NOTE: Multi select
2695	"accessed or impacted flags".)
2696	A. Personally Identifying Numbers (DESIGN NOTE: Multi select and for sub questions
2697	"a., b., c.", repeated for each response selected)

⁶⁰ **Impact**: is defined by CDM as "the loss of confidentiality, integrity, or availability that could be expected to have an adverse effect on organizational operations or organizational assets or individuals (CDM Glossary of Terms).

2698	1. Full social security number
2699	a. Provide count
2700	b. Is this count known or approximate? (Known/Approximate)
2701	c. Did potential or confirmed access occur? (Potential/Confirmed)
2702	2. Truncated or partial social security number
2703	3. Driver's license number
2704	4. License plate number
2705	5. Drug Enforcement Administration (DEA) registration number
2706	6. File/case identification (ID) number
2707	7. Patient ID number
2708	8. Health plan beneficiary number
2709	9. Student ID number
2710	10. Federal student aid number
2711	11. Passport number
2712	12. Alien registration number
2713	13. Department of Defense (DOD) ID number
2714	14. DOD benefits number
2715	15. Employee Identification Number
2716	16. Professional license number
2717	17. Taxpayer Identification Number
2718	18. Business Taxpayer Identification Number (sole proprietor)
2719	19. Credit/debit card number
2720	20. Business credit card number (sole proprietor)
2721	21. Vehicle Identification Number
2722	22. Business Vehicle Identification Number (sole proprietor)
2723	23. Personal bank account number
2724	24. Business bank account number (sole proprietor)
2725	25. Personal device identifiers or serial numbers
2726	26. Business device identifiers or serial numbers (sole proprietor)
2727	27. Personal mobile number
2728	28. Business mobile number (sole proprietor)
2729	29. Other (please identify)
2730	B. Biographical Information (DESIGN NOTE: Multi select and for sub questions "a., b., c.",
2731	repeated for each response selected.)
2732	1. Full name (First, Last, including nicknames)
2733	a. Provide count
2734	b. Is this count known or approximate? (Known/Approximate)
2735	c. Did potential or confirmed access occur? (Potential/Confirmed)
2736	2. Gender
2737	3. Race
2738	4. Date of birth (day, month, year)

2739	5. Ethnicity
2740	6. Nationality
2741	7. Country of birth
2742	8. City or county of birth
2743	9. State of birth
2744	10. Marital status
2745	11. Citizenship
2746	12. Immigration status
2747	13. Religion/religious preference
2748	14. Home address
2749	15. Zip code
2750	16. Home phone or fax number
2751	17. Spouse information
2752	18. Sexual orientation
2753	19. Children information
2754	20. Group/organization membership
2755	21. Military service information
2756	22. Mother's maiden name
2757	23. Business mailing address (sole proprietor)
2758	24. Business phone or fax number (sole proprietor)
2759	25. Global positioning system (GPS)/location data
2760	26. Personal email address
2761	27. Business email address
2762	28. Employment information
2763	29. Personal financial information (including loan information, but not including
2764	account or payment card numbers)
2765	30. Business financial information (including loan information, but not including
2766	account or payment card numbers)
2767	31. Alias (i.e., username or screenname)
2768	32. Education information
2769	33. Resume or curriculum vitae (DISPLAY NOTE: If these documents include additional
2770	types of PII, e.g., address or SSN, please indicate those fields separately.)
2771	34. Professional/personal references (DISPLAY NOTE: If these documents include
2772	additional types of PII, e.g., address or SSN, please indicate those fields separately.)
2773 C.	Biometrics, Distinguishing Features, and Characteristics (Design NOTE"
2774	Multi select and for sub questions "a., b., c.", repeated for each response selected.)
2775	1. Filigerprints
2770	a. Provide count b. La this count known or enprovingets? (Vnown/Approvingets)
2777	 Did notantial or confirmed cocces cocur? (Detential/Coeffirmed)
2770	c. Did potential or confirmed access occur? (Potential/Confirmed)
2779	2. Paim prints

2780	3. Vascular scans
2781	4. Retina/iris scans
2782	5. Dental profile
2783	6. Scars, marks, tattoos
2784	7. Hair color
2785	8. Eye color
2786	9. Height
2787	10. Video recording
2788	11. Photos
2789	12. Voice/audio recording
2790	13. DNA sample or profile
2791	14. Signatures
2792	15. Weight
2793	D. Medical/Health and Emergency Information (DESIGN NOTE: Multi select and
2794	for sub questions "a., b., c.", repeated for each response selected.)
2795	1. Physical medical/health information
2796	a. Provide count
2797	b. Is this count known or approximate? (Known/Approximate)
2798	c. Did potential or confirmed access occur? (Potential/Confirmed)
2799	2. Mental health information
2800	3. Disability information
2801	4. Workers' compensation information
2802	5. Patient ID number
2803	6. Emergency contact information
2804	E. Device Information (DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated
2805	for each response selected.)
2806	1. Device settings or preferences (e.g., security level, sharing options,
2807	ringtones)
2808	a. Provide count
2809	b. Is this count known or approximate? (Known/Approximate)
2810	c. Did potential or confirmed access occur? (Potential/Confirmed)
2811	2. Cell tower records (i.e., logs, user location, time, etc.)
2812	3. Network communications data
2813	F. Other Specific Information or File Types (DESIGN NOTE: Multi select and for sub
2814	questions "a., b., c.", repeated for each response selected.)
2815	1. Taxpayer information/Tax return information
2816	a. Provide count
2817	b. Is this count known or approximate? (Known/Approximate)
2818	c. Did potential or confirmed access occur? (Potential/Confirmed)
2819	2. Law enforcement information
2820	3. Security clearance/background check information

2821	4. Civil/criminal history information/police record
2822	5. Academic and professional background information
2823	6. Health information
2824	7. Case files
2825	8. Personnel files
2826	9. Credit history information
2827	10. Other
2828	a. Please provide the other specific information or file type(s)
2829	Incident Stage (A): Security Control(s) [Contributing to
2830	Incident]
2831	79. [Op] + [RR but NOT FISMA or FedRAMP reporting] Please review the "Protect"
2832	section of the CISA Cross-Sector Cybersecurity Performance Goals (CPGs). ⁶¹ To
2833	the best of your knowledge, did the implementation (or lack thereof),
2834	misconfiguration, or failure of a security control (as described in CISA's Protect
2835	CPGs). ⁶² lead to, contribute to, or otherwise factor into your incident? (Yes/No)
2836	A. Yes
2837	i. (DESIGN NOTE: If Yes) Select all that apply [] non-implementation []
2838	misconfiguration and/or [] failure of the security control
2839	B. No
2840	C. Unknown (DESIGN NOTE: If the person selects "Unknown", then DISPLAY NOTE: When and if,
2841	during your investigation, you discover knowledge about security controls contributing to the
2843	the implementation (or lack thereof), improper configuration, or other aspect of the control led to,
2844	contributed to, or otherwise factored into the incident.)
2845	80. {Conditional if $Q 79 = Yes$ } [Op] + [RC] Select the applicable control(s) from the
2846	CISA Cybersecurity Performance Goals, "Protect" section ⁶³ .
2847	A. Select from [DESIGN NOTE: See Appendix 2 for answer options, multi choice select) (DESIGN
2848	NOTE: Repeat for each CPG Protect Control selected)
2849	1. (DISPLAY NOTE: Select one) Was the [] failure, [] misconfiguration, or []non-
2850	implementation of the control due to a published $\text{CVE}^{64}(s)$?
2851	a. Yes (DESIGN Note: The following "CVE" questions are conditional only if the
2852 2052	reporter selected "YES" to security controls factoring into the incident) 1 = What is the CVE(s)?
2854	(DESIGN NOTE: Multi select for Failed, Misconfigured, and Not
2855	implemented) (repeat for each CVE identified)

⁶¹ Cross-Sector Cybersecurity Performance Goals | CISA (https://www.cisa.gov/cross-sector-cybersecurity-

performance-goals)
 ⁶² See Appendix 2
 ⁶³ See Appendix 2
 ⁶⁴ Common Vulnerabilities and Exposures (CVE) is a program that identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities.

2857c. Unknown28582. Do one or more of the observed TTPs reported earlier in this report related2859this selected security control? (Yes/No)2860a. (DESIGN NOTE: If Yes) Please select from your reported observed2861TTPs those that are attributed to this security control (DESIGN NOTE)	O TE:
28582. Do one or more of the observed TTPs reported earlier in this report relates2859this selected security control? (Yes/No)2860a. (DESIGN NOTE: If Yes) Please select from your reported observed2861TTPs those that are attributed to this security control (DESIGN NOTE)	O TE:
2859this selected security control? (Yes/No)2860a. (DESIGN NOTE: If Yes) Please select from your reported observed2861TTPs those that are attributed to this security control (DESIGN NO	TE:
2860a.(DESIGN NOTE: If Yes) Please select from your reported observed2861TTPs those that are attributed to this security control (DESIGN NO	TE:
2861 TTPs those that are attributed to this security control (DESIGN NO	TE:
2862 Display all TTPs [MITRE ATT&CK and general] that have been reported and	
2863 allow user to select one or more TTPs and associate with this/these security	
2864 control(s).)	
B. Please provide any additional information regarding how security control	
2866 implementation, failure, misconfiguration, or non-implementation played a role	in
2867 this incident (DESIGN NOTE: Open text) (DISPLAY NOTE: This includes not only any addition	nal
2868 information regarding how failure, misconfiguration, or non-implementation of a control may have	
2869 contributed to an incident, but also information regarding any controls that were also effective in	
28/0 mitigating or detecting the incident, and/or controls that worked and forced the threat actor to pive	t to
2871 someting more complex, etc.)	
2872 81 [FISMA or FodRAMP reporting only] (DISPLAY NOTE: CISA understands the NIST SI	
287.4 800.53 and NIST SP 800.171 are primary sources to follow when establishing and setting various system	
2875 controls under FISMA and FedRAMP requirements. CISA also acknowledges others outside FISMA at	d
2876 FedRAMP may not be as familiar with these publications. Therefore, CISA has implemented two paths	u for
2877 identifying security controls that have contributed to the incident. For FISMA and/or FedRAMP report	ing
2878 the NIST publications are available to reference. For all other reporting, the "Protect" section of the CI	SA
2879 Cross-Sector Cybersecurity Performance Goals (CPGs). ⁶⁵ will be referenced.) To the best of your	
2880 knowledge, did the implementation (or lack thereof), misconfiguration, or failure of	f a
2881 security control (as described in NIST SP 800-53) lead to, contribute to, or otherwi	se
2882factor into your incident? (Yes/No)	
2883 A. Yes	
2884 i. (DESIGN NOTE: If Yes) Select all that apply [] non-implementation []	
2885 misconfiguration and/or [] failure of the security control	
2886 B. No	
2887 C. Unknown (DESIGN NOTE: If the person selects "Unknown", then DISPLAY NOTE: When an	d if,
2888 during your investigation you discover knowledge about security controls contributing to the incid	ent,
2889 please return to this question and share any details you can about security controls where the	
2890 implementation (or lack thereof), improper configuration, or other aspect of the control led to,	
2891 contributed to, or otherwise factored into the incident.) 2002 (Conditional if () 21 - Vec) [FISMA and FedDAMD ankyl (MODE AV NOTE T	
2892 δ_{2} . {Conditional II Q $\delta_{1} = 1 \text{ es}$ } [FISWIA and FedKAWIP ONIY] (DISPLAY NOTE: To	
2893 enhance trends and analysis of security controls between incidents, establishing a common reference is a 2804 sound approach. Therefore, CISA has associated the CISA CPCs with a subset of NIST SP 800.53 controls and analysis of security controls between incidents, establishing a common reference is a 2804 sound approach.	ola
2895 (NIST SP 800-171 is in development). You will have an opportunity to select this subset first if applicable	e.
2896 then can select from the remaining NIST SP 800-53 set of controls if necessary.) Select the applicab	le
2897 control(s) from NIST SP 800-53 (CPG preferred list first), then if applicable select	
2898 from the remaining controls.	

⁶⁵ <u>Cross-Sector Cybersecurity Performance Goals | CISA</u> (<u>https://www.cisa.gov/cross-sector-cybersecurity-performance-goals</u>)

2899	
2900	A. Select from (DESIGN NOTE: provide NIST SP 800-53 subset list per Appendix 2 CPG to NIST SP
2901	800-53 mapping as first dropdown list, then provide another dropdown list identifying remaining
2902	NIST SP 800-53 controls) (DESIGN NOTE: Repeat for each control selected, multi choice select)
2903	1. (DISPLAY NOTE: Select one) Was the [] failure, [] misconfiguration, or []non-
2904	implementation of the control due to a published CVE ⁶⁶ (s)?
2905	a. Yes (DESIGN Note: The following "CVE" questions are conditional only if the
2906	reporter selected "YES" to security controls factoring into the incident)
2907	1. What was the CVE(s)?
2908	(DESIGN NOTE: Multi select for Failed, Misconfigured, and Not
2909	implemented) (repeat for each CVE identified)
2910	b. No
2911	c. Unknown
2912	2. Does one or more of the observed TTPs reported earlier in this report relate
2913	to this selected security control? (Yes/No)
2914	a. (DESIGN NOTE: If Yes) Please select from your reported observed
2915	TTPs the one(s) that are attributed to this security control (DESIGN
2916	NOTE: Display all TTPs [MITRE ATT&CK and general] that have been reported
2917	and allow user to select one or more TTPs and associate with this/these security
2918	control(s).
2919	B. Please provide any additional information regarding how security control
2920	implementation, failure, misconfiguration, or non-implementation played a role in
2921	this incident (DESIGN NOTE: Open text) (DISPLAY NOTE: This includes not only any additional
2922	information regarding how failure, misconfiguration, or non-implementation of a control may have
2923	contributed to an incident, but also information regarding any controls that were also effective in
2924 2925	mitigating or detecting the incident, and/or controls that worked and forced the threat actor to pivot to something more complex etc.)
2926	something more complex, etc.)
2320	
2027	o Containment (C) Stage 67
2927	0. Contamment (C) Stage
2928	83. [Op] + [FISMA Req] Have you begun the containment stage? (Yes/No/Unsure)
2929	(Note: This stage involves taking steps to prevent the incident from spreading
2930	further.)
2931	A. (DESIGN NOTE: If Yes) Provide the date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
2932	offset>) containment activities began
2933	B. Provide an overview of your containment strategy
	· · · · · · · · · · · · · · · · · · ·

⁶⁶ Common Vulnerabilities and Exposures (CVE) is a program that identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities.

https://cve.mitre.org/

⁶⁷ Containment Stage – Stage of the incident life cycle that employs activities before an "incident overwhelms resources or increases damage. Containment provides time for developing a tailored remediation strategy" and can involve many different approaches based on the known severity of the incident as determined during the Analysis Stage "(e.g., shut down a system, disconnect it from a network, disable certain functions)." [derived from pg 35 of NIST 800-61 r2]

2934	1. If implementation of the containment strategy is complete, was the
2935	containment strategy successful? (Y/N)
2936	a. (DESIGN NOTE: If N_0) Provide details on how your strategy is
2937	changing (DESIGN NOTE: Open text)
2938	84. [CUI] {Conditional} [Op] + FISMA Req] What specific containment action(s) have
2939	been taken? (DESIGN NOTE: Can be more than one, include options to add)
2940	A. Description (DESIGN NOTE: Open text)
2941	B. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
2942	C. Has this action been completed? (Yes/No)
2943	1. (DESIGN NOTE: If Yes) Was this action successful? (Yes/No)
2944	a. (DESIGN NOTE: If No) Can you identify why it wasn't successful?
2945	(DESIGN NOTE: Open text)
2946	b. [CUI] (DESIGN NOTE: If No) Provide details on how your
2947	containment action is changing (DESIGN NOTE: Open text)
2948	85. [RC] Have you completed containment? (Yes/No)
2949	
2950	Incident Stage (C): Countermeasures – Containment
2951	86. [Op] + [FISMA Req] As explained earlier, the MITRE D3FEND matrix categorizes
2952	countermeasures into multiple categories. Containment actions are identified in the
2953	"harden," "isolate," and "deceive" categories. Please select the containment actions
2954	you have taken from among these categories. (Select all that apply)
2955	A. Select applicable "containment" counter measures from the MITRE D3FEND list

A. Select applicable "containment" counter measures from the MITRE D3FEND list:

ATT&CK	Lookup			Search D	3FEND's 618	Artifacts			D3FE	ND Looku	ıp
Model	-	Hai	den		Detect	- Iso	olate	- Dece	eive	Evict	Restor
+	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	+	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	+	+
	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication		Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet	Decoy File		
	Dead Code Elimination	Certificate- based Authentication	Message Encryption	Disk Encryption		Executable Denylisting	DNS	Integrated Honeynet	Decoy Network Resource		
	Exception Handler	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking		Hardware- based Process	DNS Denylisting	Standalone Honeynet	Decoy Persona		
	Pointer Validation	Credential Rotation		File Encryption		ISOlation IO Port Restriction	Forward Resolution Domain		Decoy Public Release		
	Authentication	Credential		Local File Permissions		Kernel	Denylisting		Decov		
	Process Segment	Scoping		RF Shielding		based Process	Hierarchical Domain Depylisting		Session Token		
	Prevention	Domain Trust Policy		Software		Mandatory	Homoglyph		Decoy User		
	Segment Address Offset	Multi-factor Authentication		System		Access Control	Ecoward		Credential		
	Stack Frame Canary	One-time Password		Configuration Permissions		System Call Filtering	Resolution IP Denylisting				
	Validation	Strong		TPM Boot Integrity			Reverse				
		Password Policy					IP Denylisting				
		User Account Permissions					Encrypted Tunnels				
							Network Traffic Filtering				
							Inbound Traffic Filtering				
							Email Filtering				
							Outbound				

2956	
2957	
2958	B. [Op] We are unable to use MITRE D3FEND to identify "containment"
2959	countermeasures used during this incident, or our organization leveraged a
2960	"containment" countermeasure not listed or that is currently unidentified in
2961	MITRE D3FEND
2962	1. Did you employ a containment technique that potentially fit within an
2963	existing "MITRE D3FEND tactic" but was not listed? (Yes/No) (DISPLAY
2964	NOTE: The top-line categories associated with containment are "harden", "isolate", or
2965	"deceive". These are considered the "tactics".)
2966	(DESIGN NOTE: If Yes)
2967	a. Which tactic did your containment action fall under?
2968	1. Harden
2969	i. Which base technique did your action fall under?
2970	1. Application hardening
2971	2. Credential hardening
2972	3. Message hardening

2973	4. Platform hardening
2974	2. Isolate
2975	i. Which base technique did your action fall under?
2976	1. Execution isolation
2977	2. Network isolation
2978	3. Deceive
2979	i. Which base technique did your action fall under?
2980	1. Decoy environment
2981	2. Decoy object
2982	b. Description (DESIGN NOTE: Open text)
2983	2. (DESIGN NOTE: If N_0) If unable to use MITRE D3FEND to identify
2984	"containment" countermeasures used during this incident and cannot bucket
2985	the countermeasure into an existing MITRE D3FEND category, please
2986	provide a description and details of the countermeasures you have employed
2987	(DESIGN NOTE: Open text)
2988	C. Unknown
2989	D. None
2990	87. [Op] Please provide any additional context for the "containment" countermeasures
2991	you have taken (DESIGN NOTE: Open text)
2992	p.Eradication Stage ⁶⁸ (E)
2993	88. [CUI] [Op] + [FISMA Req] Have you begun the eradication stage? (Yes/No/Unsure)
2994	A. [If Yes] Provide the date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
2995	eradication activities began.
2996	1. [CUI] {Conditional} [Op] + [FISMA Req] Provide an overview of your
2997	eradication strategy (DESIGN NOTE: Open text)
2998	2. {Conditional} [Op] + [FISMA Req] Have you completed the eradication
2999	activities? (Yes/No)
3000	a. (DESIGN NOTE: If Yes) Please provide date and time (yyyy-mm-dd
3001	HH:MM - <utc offset="">)</utc>
3002	b. (DESIGN NOTE: If N_0) Is the implementation of your eradication
3003	strategy complete? (Y/N)
3004	c. (DESIGN NOTE: If N ₀) Was the eradication strategy successful? (Y/N)

⁶⁸ Eradication Stage: Stage of the incident life cycle the follows one or more containment activities and results of further analysis that "may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated [and remove any remnants of invalid computer code, invalid system accounts and other threat actor influenced system configurations to eliminate the threat.] For some incidents, eradication is either not necessary or is performed during recovery (e.g., files are restored from valid backups)." [derived from pg. 37 of NIST 800-61 r2]

3005	1. (DESIGN NOTE: If N_0) Provide details on how your eradication					
3006	strategy is changing (DESIGN NOTE: Open text)					
3007	d. (DESIGN NOTE: If N_0) What specific eradication action(s) have been					
3008	taken? (DESIGN NOTE: Can be more than 1, include options to add)					
3009	1. Description (DESIGN NOTE: Open text)					
3010	2. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>					
3011	3. Has this action been completed? (Yes/No)					
3012	i. (DESIGN NOTE: If Yes) Was this action successful? (Yes/No)					
3013	ii. (DESIGN NOTE: If No) Can you identify why it wasn't					
3014	successful?					
3015	iii. (DESIGN NOTE: If No) Provide details on how your					
3016	eradication action is changing.					
3017	7					
3018	Incident Stage (E): Countermeasures – Eradication					
3019	89. [Op] + [FISMA Req] As noted earlier, the MITRE D3FEND matrix categorizes					
3020	countermeasures into multiple categories. Eradication actions are identified in					
3021	MITRE's D3FEND matrix in the "evict" category. Please select the eviction actions					
3022	you have taken from this category (Select all that apply.					
3023	A Select applicable "evict" counter measures from the MITRF D3FFND list					

A. Select applicable "evict" counter measures from the MITRE D3FEND list:



3025	
3026	B. [Op] We are unable to use MITRE D3FEND to identify eradication counter
3027	measures used during this incident, or our organization leveraged an eradication
3028	counter measure not listed or that is currently unidentified in MITRE D3FEND.
3029	1. Did you employ a eradication technique that potentially fit within an existing
3030	"MITRE D3FEND tactic" but was not listed? (Yes/No) (DISPLAY NOTE: The
3031	top-line category associated with eradication is: "evict". This is considered the "tactics")
3032	(DESIGN NOTE: If Yes) Which evict technique did you action fall under?
3033	1. Credential eviction
3034	i. Description

3035	2. File eviction						
3036	i. Description						
3037	3. Process eviction						
3038	i. Description						
3039	2. Please provide a description and details of the counter measures you have						
3040	employed (DESIGN NOTE: Open text)						
3041	C. (DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify "eradication"						
3042	counter measures used during this incident and cannot bucket the counter measure						
3043	into an existing MITRE D3FEND category, please provide a description and						
3044	details of the counter measures you have employed (DESIGN NOTE: Open text)						
3045	D. Unknown						
3046	E. None						
3047	90. [CUI] {Conditional} [Op] + [FISMA Req] Please provide any additional context for						
3048	the "eradication" actions you have taken (DESIGN NOTE: Open text)						
3049	q. Recovery (R) Stage ⁶⁹						
3050	91. [CUI] [Op] + [FISMA Req] Have you begun the recovery stage? (Yes/No/Unsure)						
3051	(DISPLAY NOTE: In the recovery stage, the focus is on restoring affected systems and services to normal						
3052	operation.)						
3053	A. [RC] (DESIGN NOTE: If Yes)						
3054	1. Provide the date and time (yyyy-mm-dd HH:MM - <utc>) Please enter the</utc>						
3055	organization's estimated recovery date and time						
3056	a. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>						
3057	2. [Op] + FISMA Req] Describe your recovery strategy (DESIGN NOTE: open text)						
3058	3. [Op] + [FISMA Req] Have you completed the recovery stage and "accepted"						
3059	normal operations resumed? (Yes, No)?						
3060	a. (DESIGN NOTE: If Yes) Please provide the Date and Time (yyyy-mm-						
3061	dd HH:MM - <utc offset="">)</utc>						
3062							
3063	4. Was the recovery strategy successful? (Yes/No)						
3064	(DESIGN NOTE: If No)						
3065	a. Did you modify your strategy after you began recovery? (Yes/No)						
3066	[CUI] (DESIGN NOTE: If Yes) Why did you modify the strategy?						
3067	(DESIGN NOTE: Open text)						
3068							

⁶⁹ Recovery Stage - Stage in the Incident Life cycle that provides "restoration of critical information technology systems and services" to normal [or newly accepted] operations and within an accepted (by the owning entity) time period. "Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists)." [derived from "intermediate recovery". page 347 of https://www.dhs.gov/publication/dhs-lexicon and pg. 37 of NIST 800-61 r2]

3069	92. [Op] + [RR] Estimate the scope of resources needed to recover from the incident
3070	(recoverability).
3071 3072	A. Regular (DISPLAY NOTE: (Provide hover-over) Time to recover is predictable with existing resources.)
3073 3074	B. Supplemented (DISPLAY NOTE: (Provide hover-over) Time to recover is predictable with additional resources.)
3075 3076	C. Extended (DISPLAY NOTE: (Provide hover-over) Time to recover is unpredictable; additional resources and outside help are needed.)
3077 3078	D. Not recoverable (DISPLAY NOTE: (Provide hover-over) Recovery from the incident is not possible (i.e., sensitive data exfiltrated and posted publicly).)
3079	
3080	Incident Stage (R): Recovery Actions
3081	93. [Op] + [FISMA Req] As noted earlier, the MITRE D3FEND matrix categorizes
3082	countermeasures into multiple categories. Recovery activities are identified in

3083MITRE's D3FEND matrix in the "restore" category. Please select the recovery3084actions you have taken from this category. Select all that apply.

3085

A. Select applicable "restore" measures from the MITRE D3FEND list:



3086	Sonware
3087	B. [Op] We are unable to use MITRE D3FEND to identify "recovery"
3088	countermeasures used during this incident, or our organization leveraged a
3089	"recovery" counter measure not listed or that is currently unidentified in MITRE
3090	D3FEND.
3091	1. Did you employ a recovery technique that potentially fit within an existing
3092	"MITRE D3FEND tactic" but was not listed? (Yes/No) (DISPLAY NOTE: The
3093	top-line category associated with "recovery" is: "restore." This is considered the "tactic"),
3094	(DESIGN NOTE: If Yes) Which restore technique did your action(s) fall under:
3095	1. Restore access
3096	i. Description

3097	2. Restore object							
3098	i. Description							
3099	2. (DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify							
3100	"recovery" countermeasures used during this incident, and you cannot bucket							
3101	vour counter measure into an existing MITRE D3FEND category. nlease							
3102	provide a description and details of the counter measures you have employed							
3103	(DESIGN NOTE: Open text)							
3104	C. Unknown							
3105	D. None							
3106	94. [Op] + [FISMA Reg] Please describe any additional recovery steps you have taken							
3107	(e.g., additional external outreach and/or support, update any relevant policies.							
3108	procedures and plans such as incident response plans continuity of business plans							
3100	disaster recovery plans, system back-up and restore plans, business everyise plans,							
3110	(DESIGN NOTE: Onen text)							
3111								
-								
3112	r. Post-Incident (P-I) Stage							
3113	95. [Op] + [FISMA Req] Has the incident concluded? (Yes/No)							
3114	(DESIGN NOTE: If Yes) Provide your post incident report/details							
3115	A. [Op] + [FISMA Req] If available, submit any post incident or after-action reports							
3116	related to this incident (Submit your organization's post incident report (WITH AN UPLOAD FILE							
3117	OPTION HERE.) (DISPLAY NOTE: For Federal civilian executive branch agencies, this is in line with CISA's Incident Playbook to allow CISA to "validate organization's response") ⁷⁰							
3119	B [On] + [FISMA Real Looking back on your incident response, was there							
3120	information that, had you received it or learned it sooner, would have led to a							
3121	more streamlined quicker and/or more effective incident response? If yes							
3121	identify the incident response state where you would have preferred to receive							
3122	this information (DESICN NOTE: Multi select; based on NIST 800.61 r ² , the major phases of an							
3123	incident life cycle.)							
3125	1. Identification and detection							
3126	a Which organization could have provided the information? (DESIGN)							
3127	NOTE: Repeated for each stage selected.)							
3128	2. Analysis							
3129	3. Containment							
3130	4. Eradication							
3131	5. Recovery							
3132	6. Post-incident							

⁷⁰ Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems: Publication: November 2021

3133	C. [Op] + [FISMA Req] Has the impacted organization performed a review of the
3134	incident and incident response to identify lessons learned? (Y/N)
3135	1. (DESIGN NOTE: If Yes) Please describe the identified lessons learned in the areas
3136	of:
3137	a. Incident handling processes
3138	b. Mean time to effective analysis
3139	c. Mean time to detection
3140	d. Mean time to response
3141	e. Mean time to defense
3142	f. Mean time to reporting
3143	g. Other
3144	D. [Op] + [FISMA Req] Based on your experience in this incident, please provide
3145	recommendations on how CISA can improve the support it provides
3146	1. What could CISA do differently in future incidents? (DESIGN NOTE: Open text)
3147	2. Are there indicators of compromise or relevant detection mechanisms you
3148	have not provided previously in this report and believe can enable detection
3149	of similar incidents in the future? (DESIGN NOTE: Open text)
3150	3. What additional tools or resources would you need to detect, analyze, and
3151	mitigate future incidents? (DESIGN NOTE: Open text)
3152	

s. Event Reporting (Below Incident Thresholds)

3154 (FISMA – Only)

3155	(DESIGN NOTE: FISMA Only – If reporter answers "NO" to all CIA Impact Assessments)
	Confidentiality, Integrity, Availability Assessment ²⁰
	21. [RA] (DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event- Incident FLAC for FISMA reporters only. If O21 A C are anywarded "no" that terminates the test of the
	Incident Questions for a FISMA reporter, and the FISMA reporter is directed towards filling out "Event
	Reporting " only.) At this time, is this incident known to either imminently ²¹ or <u>actually</u>
	information or an information system (select all that apply). (DESIGN NOTE: For non-
	FISMA reports, there must be at least one selection from CIA below that is either "imminently" or
	"unsure" or "none", then the event does NOT meet threshold for an "Incident". Consider, if all non-FISMA
	reports select "unsure/None" for all three CIA questions, then DISPLAY NOIE: You have not indicated an impact to at least one of the three areas of confidentiality, integrity, or availability per the definition of an
	incident.) A confidentiality ²² [] imminently: [] actually: [] unsure []/none (DESIGN NOTE: Have
	radio button for all)
	B. integrity, ²³ [] imminently; [] actually; [] unsure/none (DESIGN NOTE: Have radio button for all)
3156	C. availability ²⁴ [] imminently; [] actually; [] unsure/none (DESIGN NOTE: Have radio button for all)
3157	96. [FISMA Req] Has this activity already been reported? (Yes/No)
3158	A. (DESIGN NOTE: If Yes) Provide
3159	1. Incident report form submission number.
3160	2. CISA incident tracking number.
3161	97. [CUI] [FISMA Req] Describe the scope of impacted systems and provide a high-level
3162	summary of the event activity. (DESIGN NOTE: Narrative of the event detection)
3163	98. [FISMA Req] When did you first detect the activity?
3164	A. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
3165	99. [FISMA Req] When did you declare an event?
3166	A. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
3167	100. [FISMA Req] Please provide any additional information relevant to the event
3168	(DESIGN NOTE: Open text)
3169	101. [FISMA Req] Has the entity covered by this event resolved the consequences for
3170	the event? (Yes/No)
3171	A. (DESIGN NOTE: If Yes) Provide the date and time when the event was resolved
3172	1. Recovered as of date/time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
3173	102. [FISMA Req] Please describe any additional steps you have taken to resolve the
3174	event (e.g., additional external outreach and/or support, update any relevant policies,
3175	procedures, and plans, such as incident response plans, continuity of business plans,
3176	disaster recovery plans, system back-up and restore plans, business exercise plans)
3177	(DESIGN NOTE: Open text)

t. Data Marking Stage 3178

3179	Cybersecurity Information Sharing Act of 2015				
3180	Acknowledgement				
3181	(DESIGN NOTE: Only Show for Non-Federal Voluntary Reporters [i.e., Voluntary Report] or Non-				
3182	Federal Non-Voluntary Reporters [e.g., TSA], not to be shown for FISMA reporters)				
3183	103. [Op] + [Not Applicable to FISMA Reporting] To the extent not already indicated				
3184	using the data markings, do your responses to any of the questions above constitute				
3185	cyber threat indicator(s) or defensive measure(s) submitted under the Cybersecurity				
3186	Information Sharing Act of 2015 that the submitter is requesting be treated as				
3187	commercial, financial, and proprietary? (Yes/No)				
3188	A. (DESIGN NOTE: If Yes) Select question numbers (DESIGN NOTE: Provide drop-down, multi				
3189	select).				
3190					
3191	Overall Report Data Markings				
3192	104. [CUI] [Op] + [RR] The most restrictive marking that has been reported in this				
3193	incident is X. ⁷¹ Is this a valid marking for the entire incident? (Yes/No)				
3194	A. (DESIGN NOTE: If Yes) Then the incident marking is X. ⁷²				
3195	B. (DESIGN NOTE: If No) User to enter new marking for the entire incident				
3196	(DESIGN NOTE: See Appendix 1 for question options. ⁷³)				
3197					
3198	u.End of Incident Reporting Questions				
3199					
3200	v. Appendix 1: Data Marking				
3201	Data Marking Options				
3202					
3203	1. Specific data marking options are as follows				
3204	1. [C-15] Cybersecurity Information Sharing Act of 2015 commercial, financial, and				
3205	proprietary. ⁷⁴				
3206	2. [CUI] Controlled unclassified information (CUI). ⁷⁵				

⁷¹ The default data marking presented here.
⁷² The accepted default data marking here.
⁷³ Option to change default data marking.

⁷⁴ Indicating that the marked data constitutes cyber threat indicator(s) or defensive measure(s) submitted under the Cybersecurity Information Sharing Act of 2015 that the submitter is requesting be treated as commercial, financial, and proprietary.

⁷⁵ CUI Markings | National Archives

w. Appendix 2: CISA Cybersecurity Performance Goals.⁷⁶ (Protect) & NIST SP 800-53 References

3210

3211

Protect CISA CPGs & NIST SP 800-53 References

CPG	Additional	Security	Outcome	TTP or Risk	Recommended Action
#	Reference(s)	Practice		Addressed	
	[including				
	NIST 800-53				
	for FISMA				
	reports]				
2.A	NIST SP 800-	Changing	Prevent threat	Valid accounts -	An enforced organization-wide policy
	53: IA-5	default	actors from using	default accounts	and/or process that requires changing
	ISA 62443-2-	passwords	default passwords	(T1078.001)	default manufacturer passwords for
	1:2009 4.3.3.5.1		to achieve initial	Valid accounts (ICS	any/all hardware, software, and
	ISA 62443-3-		access or move	T0859)	firmware before putting on any
	3:2013 SR 1.1,		laterally in a		internal or external network. This
	SR 1.2, SR 1.3,		network.		includes IT assets for operational
	SR 1.4, SR 1.5,				technology, such as operational
	SR 1.7, SR 1.8,				technology administration web pages.
	SR 1.9				
					In instances where changing default
					passwords is not feasible (e.g., a
					control system with a hard-coded
					password), implement and document
					appropriate compensating security
					controls, and monitor logs for
					network traffic and login attempts on
					those devices.
					One metional technology, While
					operational technology: while
)	organization's existing operational
					technology requires significantly
					more work we still recommend
					having such a policy to change
					default credentials for all new or
					future devices. This is not only easier
					to achieve, but also reduces potential
					risk in the future if adversary TTPs
					change.

⁷⁶ <u>Cross-Sector Cybersecurity Performance Goals | CISA (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)</u>

1						
	2.B	NIST SP 800- 53: IA-5 ISA 62443-2- 1:2009 4.3.3.5.1 ISA 62443-3- 3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 XKCD 936	Minimum password strength	Organizational passwords are harder for threat actors to guess or crack.	Brute force - password guessing (T1110.001) Brute force - password cracking (T1110.002) Brute force - password spraying (T1110.003) Brute force - credential stuffing (T1110.004)	Organizations have a system- enforced policy that requires a minimum password length of 15* or more characters for all password- protected IT assets and all operational technology assets, when technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.
						This goal is particularly important for organizations that lack widespread implementation of multifactor authentication (MFA) and capabilities to protect against brute- force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods.
						* Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember.
						** Operational technology assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk operational technology assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or on wind turbines.
	2.C	NIST SP 800- 53: AC-2, AC-3 ISA 62443-2- 1:2009 4.3.3.5.1 ISA 62443-3- 3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	Unique credentials	Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and operational technology networks	Valid accounts (T1078, ICS T0859) Brute force - password guessing (T1110.001)	Organizations provision unique and separate credentials for similar services and asset access on IT and operational technology networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.

2.D	NIST SP 800- 53: AC-2, AC-3 ISA 62443-2- 1:2009 4.3.3.5.1 ISA 62443-3- 3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	Revoking credentials for departing employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Valid accounts (T1078, ICS T0859)	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.
2.E	NIST SP 800- 53: AC-6 ISA 62443-2- 1:2009 4.3.3.7.3 ISA 62443-3- 3:2013 SR 2.1	Separating user and privileged accounts	Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.	Valid accounts (T1078, ICS T0859)	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are revaluated on a recurring basis to validate continued need for a given set of permissions.
2.F	NIST SP 800- 53: AC-4, SC- 7, SI-4 ISA 62443-2- 1:2009 4.3.3.4 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 6.2, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A 14 1.3	Network segmentation	Reduce the likelihood of adversaries accessing the operations technology network after compromising the IT network.	Network service discovery (T1046) Trusted relationship (T1199) Network connection enumeration (ICS T0840) Network sniffing (T1040, ICS T0842)	All connections to the operational technology network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and operational technology networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.
2.G	NIST SP 800- 53: AC-7 ISA 62443-2- 1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3- 3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10	Detection of unsuccessful (automated) login attempts	Protect organizations from automated, credential-based attacks.	Brute force - password guessing (T1110.001) Brute force - password cracking (T1110.002) Brute force - password spraying (T1110.003) Brute force - credential stuffing (T1110.004)	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins over a 10-minute period.

2.H	NIST SP 800- 53: IA-2, IA-3 ISA 62443-2- 1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3- 3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10	Phishing- resistant MFA	Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.	Brute force (T1110) remote services - Remote desktop protocol (T1021.001) Remote services - SSH (T1021.004) Valid accounts (T1078, ICS T0859) External remote services (ICS T0822)	Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows: 1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI)-based – see CISA guidance in "Resources"); 2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used; 3. MFA via short message service (SMS) or voice only used when no other options are possible. IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems. Operational technology: Within operational technology environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible Human Machine
2.I	NIST SP 800-	Basic	Organizational	User training (M1017,	At least annual trainings for all
	53: AT-2 ISA 62443-2-	cybersecurity training	users learn and perform more	ICS M0917)	organizational employees and contractors that cover basic security
	1:2009 4.3.2.4.2	6	secure behaviors		concepts, such as phishing, business
	27001:2013				security, password security, etc., as
	A.7.2.2, A.12.2.1				well as foster an internal culture of security and cyber awareness.
-	1.12.2.1				New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.
2.J	NIST SP 800- 53: AT-3	Operational technology	responsible for	User training (M1017, ICS M0917)	In addition to basic cybersecurity training, personnel who maintain or
	ISA 62443-2- 1:2009	cybersecurity training	securing operational		secure operational technology as part of their regular duties receive
	4.3.2.4.2,		technology assets		operational technology-specific cybersecurity training on at least an
	ISO/IEC		specialized		annual basis.
	27001:2013 A.6.1.1,		operational technology-		
	A.7.2.1, A.7.2.2		focused		
			training		

2.	.K	NIST SP 800- 53: SC-8, SC- 13, SC-28 ISA 62443-3- 3:2013 SR 3.1, SR 3.4, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013	Strong and agile encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and operational technology traffic	Adversary-in-the- middle (T1557) Automated collection (T1119) Network sniffing (T1040, ICS T0842) Wireless compromise (ICS T0860) Wireless sniffing (ICS	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing
		A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3				Operational technology: To minimize the impact to latency and availability, encryption is used when feasible, usually for operational technology communications connecting with remote/external assets.
2	L	NIST SP 800- 53 Rev. 4 AC- 4, AC-5, AC-6, MP-12, PE-19, PS-3, PS-6, SC- 7, SC-8, SC-11, SC-12, SC-13, SC-28, SC-31, SI-4 ISA 62443-3- 3:2013 SR 3.4, SR 4.1, SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.4.2, A.9.4.4, A.9.4.5, A.10.1.1, A.11.2.1, A.13.1.3, A.13.2.1, A.13.2.1, A.13.2.4, A.14.1.2, A.1	Secure sensitive data	Protect sensitive information from unauthorized access	Unsecured credentials (T1552) Steal or forge Kerberos tickets (T1558) OS credential dumping (T1003) Data from information repositories (ICS T0811) Theft of operational information (T0882)	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.

2.M	NIST SP 800- 53 Rev. 4 AC- 4, AC-5, AC-6, CM-8, MP-6, MP-8, PE-16, PE-19, PS-3, PS-6, SC-7, SC-8, SC-11, SC-12, SC-13, SC-28, SC-31, SI-4 ISA 62443-3- 3:2013 SR 3.1, SR 3.4, SR. 3.8, SR 4.1, SR 4.1, SR 4.2, SR 5.2	Email security	Reduce risk from common email- based threats, such as spoofing, phishing, and interception	Phishing (T1566) business email compromise	On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domain-based Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies at <link bod="" to=""/> : https://www.cisa.gov/binding- operational-directive-18-01
2.N	NIST SP 800- 53: CM-10, CM-11, SC-13 ISA 62443-2- 1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3- 3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Disable macros by default	Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP	Phishing - spearphishing attachment (T1566.001) User execution - malicious File (T1204.002)	A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.
2.0	NIST SP 800- 53: CM-2, CM- 6, CM-8 ISA 62443-2- 1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3- 3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Document device configurations	More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity	Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and operational technology assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.
2.P	NIST SP 800- 53: CM-2, CM- 6, CM-8 ISA 62443-2- 1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3- 3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2.	Document Network Topology	More efficiently and effectively respond to cyberattacks and maintain service continuity	Incomplete or inaccurate understanding of network topology inhibits effective incident response and recovery	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and operational technology networks. Periodic reviews and updates should be performed and tracked on a recurring basis.

	A 12 5 1				
	A.12.5.1,				
	A.12.0.2,				
	A.14.2.2,				
	A.14.2.3,				
	A.14.2.4				
2.Q	NIST SP 800-	Hardware and	Increase visibility	Supply chain	Implement an administrative policy
	53: CM-2, CM-	software	into deployed	compromise (T1195,	or automated process that requires
	3. CM-5. CM-6.	approval process	technology assets	ICS T0862)	approval before new hardware.
	CM-10. CM-11	11 1	and reduce the	Hardware additions	firmware, or software/software
	ISA 62443-2-		likelihood of	(T1200)	version is installed or deployed
	1.2000		breach by users	Browser extensions	Organizations maintain a risk-
	1.2007		installing	(T1176)	informed allowlist of approved
	4.5.4.5.2,		instannig		handrages former and a former
	4.3.4.3.3		unapproved	Transferit cyber asset	hardware, firmware, and software
	ISA 62443-3-		nardware,	(ICS 10864)	that includes specification of
	3:2013 SR 7.6		firmware, or		approved versions, when technically
	ISO/IEC		software		feasible. For operational technology
	27001:2013				assets specifically, these actions
	A.12.1.2,				should also be aligned with defined
	A.12.5.1,				change control and testing activities.
	A.12.6.2,				
	A.14.2.2,				
	A.14.2.3,				
	A.14.2.4				
2.R	NIST SP 800-	System Backups	Organizations	Data destruction	All systems that are necessary for
	53: CP-6, CP-9,	- ,	reduce the	(T1485, ICS T0809)	operations are regularly backed up on
	CP-10		likelihood and	Data encrypted for	a regular cadence (no less than once
	ISA 62443-2-		duration of data	impact (T1486)	ner vear)
	1.2000 / 3 / 3 0		loss at loss of	Disk wine (T1561)	per year).
	1.2009 4.3.4.3.9 ISA 62443 3		service delivery	Inhibit system	Backups are stored separately from
	2.2012 CD 7 2		service derivery	minon system	the source systems and tested on a
	5:2015 SK 7.5,		or operations	$\frac{1}{1} \frac{1}{1} \frac{1}$	the source systems and tested on a
	SK /.4			Denial of control (ICS	recurring basis, no less than once per
	ISO/IEC			10813)	year. Stored information for
	27001:2013			Denial/loss of view	operational technology assets
	A.12.3.1,			(ICS 10815, 10829)	includes at a minimum:
	A.17.1.2,			Loss of availability	configurations, roles, programmable
	A.17.1.3,			(T0826)	controller (PLC) logic, engineering
	A.18.1.3			Loss/manipulation of	drawings, and tools.
				control (T0828,	
				T0831)	
2.S	NIST SP 800-	Incident	Organizations	Inability to quickly	Organizations have, maintain, update,
	53: IR-3, IR-4,	Response (IR)	maintain,	and effectively	and regularly drill IT and operational
	IR-8	Plans	practice, and	contain, mitigate. and	technology cybersecurity incident
	ISA 62443-2-		update	communicate about	response plans for both common and
	1:2009		cybersecurity	cybersecurity	organizationally-specific (e.g., by
	4.3.2.5.3.		incident response	incidents	sector, locality) threat scenarios and
	4.3.2.5.7		plans for relevant		TTPs. When conducted, tests or drills
	4.3.4.5.1		threat scenarios		are as realistic as feasible. IR plans
	434511		in our scondrios		are drilled at least annually and are
	ISA 62443_3_				undated within a risk-informed time
	3.2013 SP 3 3				frame following the lessons learned
	5.2015 SK 5.5				nortion of any everying or drill
	27001.2012				portion of any exercise of drift.
	2/001:2013				
	A.10.1.1,				
	A.17.1.1,				
	A.17.1.2,				
	A.17.1.3				

2.T	NIST SP 800- 53: AU-2, AU- 3, AU-7, AU-9, AU-11 ISA 62443-2- 1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3- 3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks	Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents Impair defenses (T1562)	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows event logging. Operational technology: For operational technology assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1				
2.U	NIST SP 800- 53: AU-2, AU- 3, AU-7, AU-9, AU-11 ISA 62443-2- 1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3- 3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	Secure Log Storage	Organizations' security logs are protected from unauthorized access and tampering	Indicator removal on host - clear Windows event logs (T1070.001) Indicator removal on host - Clear Linux or Mac system logs (T1070.002) Indicator removal on host - file deletion (T1070.004) Indicator removal on host (ICS T0872)	Logs are stored in a central system, such as a security information and event management tool or central database and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.
2.V	NIST SP 800- 53: MP-2, MP- 7 ISA 62443-3- 3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	Prohibit Connection of Unauthorized Devices	Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices	Hardware additions (T1200) Replication through removable media (T1091, ICS T0847)	Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and operational technology assets, such as by limiting use of USB devices and removable media or disabling AutoRun. Operational technology: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.

2.W	NIST SP 800-	No Exploitable	Unauthorized	Active scanning -	Assets on the public internet expose
	53: AC-4, SC-	Services on the	users cannot gain	vulnerability scanning	no exploitable services, such as
	7, SC-32, SC-	Internet	an initial system	(T1595.002)	remote desktop protocol. Where these
	39		foothold by	Exploit public-facing	services must be exposed, appropriate
	ISA 62443-3-		exploiting known	application (T1190,	compensating controls are
	3:2013 SR 3.1,		weaknesses in	ICS T0819)	implemented to prevent common
	SR 3.5, SR 3.8,		public-facing	Exploitation of remote	forms of abuse and exploitation. All
	SR 4.1, SR 4.3,		assets	service (T1210, ICS	unnecessary OS applications and
	SR 5.1, SR 5.2,			T0866)	network protocols are disabled on
	SR 5.3, SR 7.1,			External remote	internet-facing assets.
	SR 7.6			services (T1133, ICS	
	ISO/IEC			T0822)	
	27001:2013			Remote services -	
	A.13.1.1,			remote desktop	
	A.13.2.1,			protocol (T1021.001)	
	A.14.1.3				
0.37	NHOT OD 000	T • •.	D 1 .1 .1		NY 11 11 1 1
2.X	NIST SP 800-	Limit	Reduce the risk	Active scanning -	No operational technology assets are
2.X	NIST SP 800- 53: AC-4, SC-	operational	of threat actors	Active scanning - vulnerability scanning	No operational technology assets are on the public internet, unless
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC-	Limit operational technology	of threat actors exploiting or	Active scanning - vulnerability scanning (T1595.002)	No operational technology assets are on the public internet, unless explicitly required for operation.
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39	Limit operational technology connections to	of threat actors exploiting or interrupting OT	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3-	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190,	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote services (T1133, ICS	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote services (T1133, ICS T0822)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote services (T1133, ICS T0822)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote services (T1133, ICS T0822)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	NIST SP 800- 53: AC-4, SC- 7, SC-32, SC- 39 ISA 62443-3- 3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1,	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote services (T1133, ICS T0822)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).

3212

3213 x. Appendix 3: Incident Type/Categories

3214	Incident Types involving Malware (based on <u>VERIS</u> with some modifications. ⁷⁷):
3215	1. Adware
3216	2. Backdoor (enable remote access)
3217	3. Brute force attack
3218	4. Capture data from application or system process
3219	5. Capture data stored on system disk
3220	6. Client-side attack (client-side or browser attack (e.g., redirection, XSS,
3221	MitB))
3222	7. Click fraud or Bitcoin mining
3223	8. C2 (command and control)
3224	9. Destroy data (destroy or corrupt stored data)
3225	10. Disable controls (disable or interfere with security controls)
3226	11. DoS (denial of service attack)
3227	12. Downloader (pull updates or other malware)
3228	13. Exploit vulnerability in code (vs misconfiguration or weakness)

⁷⁷ Enumerations (verisframework.org)

3229	14. Export data to another site or system
3230	15. Packet sniffer (capture data from network)
3231	16. Password dumper (extract credential hashes)
3232	17. RAM scraper or memory parser (capture data from volatile memory)
3233	18. Ransomware (encrypt or seize stored data)
3234	19. Rootkit (maintain local privileges and stealth)
3235	20. Scan network (scan or footprint network)
3236	21. Spam (send spam)
3237	22. Spyware/Keylogger (spyware, keylogger or form-grabber (capture user input
3238	or activity))
3239	23. SQL injection attack
3240	24. Adminware (system or network utilities (e.g., PsTools, Netcat))
3241	25. Worm (propagate to other systems or devices)
3242	
3243	Incident Types Involving Hacking (based on <u>VERIS</u> with some modifications. ⁷⁸):
3244	1. Abuse of functionality
3245	2. Brute force or password guessing attacks
3246	3. Buffer overflow
3247	4. Cache poisoning
3248	5. Session prediction: Credential or session prediction
3249	6. CSRF: Cross-site request forgery
3250	7. XSS: Cross-site scripting
3251	8. Cryptanalysis
3252	9. DoS: Denial of service
3253	10. Foot-printing and fingerprinting
3254	11. Forced browsing or predictable resource location
3255	12. Format string attack
3256	13. Fuzz testing
3257	14. HTTP request smuggling
3258	15. HTTP request splitting
3259	16. Integer overflows
3260	17. LDAP injection
3261	18. Mail command injection
3262	19. MitM: Man-in-the-middle attack
3263	20. Null byte injection
3264	21. Offline cracking: Offline password or key cracking (e.g., rainbow tables,
3265	Hashcat, JtR)
3266	22. OS commanding

⁷⁸ Enumerations (verisframework.org)

3267	23. Path traversal
3268	24. RFI: Remote file inclusion
3269	25. Reverse engineering
3270	26. Routing detour
3271	27. Session fixation
3272	28. Session replay
3273	29. Soap array abuse
3274	30. Special element injection
3275	31. SQL injection
3276	32. SSI injection
3277	33. URL redirector abuse
3278	34. Use of backdoor or C2
3279	35. Use of stolen creds
3280	36. XML attribute blowup
3281	37. XML entity expansion
3282	38. XML external entities
3283	39. XML injection
3284	40. XPath injection
3285	41. XQuery injection
3286	42. Virtual machine escape
3287	
3288	Incident Types Involving Social Engineering (based on VERIS with some
3289	modifications. ⁷⁹):
3290	1. Baiting (planting infected media)
3291	2. Bribery or solicitation
3292	3. Elicitation (subtle extraction of info through conversation)
3293	4. Extortion or blackmail
3294	5. Forgery or counterfeiting (fake hardware, software, documents, etc.)
3295	6. Influence tactics (leveraging authority or obligation, framing, etc.)
3296	7. Scam (online scam or hoax (e.g., scareware, 419 scam, auction fraud))
3297	8. Phishing (or any type of *ishing)
3298	9. Pretexting (dialogue leveraging invented scenario)
3299	10. Propaganda or disinformation
3300	11. Spam (unsolicited or undesired email and advertisements)
3301	
3302	
3303	Incident Types Involving Misuse of Assets [sometimes called "Insider

Threats"] (based on <u>VERIS</u> with some modifications 80): 3304

 ⁷⁹ Enumerations (verisframework.org)
 ⁸⁰ Enumerations (verisframework.org)

3305	1.	Knowledge abuse: Abuse of private or entrusted knowledge
3306	2.	Privilege abuse: Abuse of system access privileges
3307	3.	Embezzlement, skimming, and related fraud
3308	4.	Data mishandling: Handling of data in an unapproved manner
3309	5.	Email misuse: Inappropriate use of email or IM
3310	6.	Net misuse: Inappropriate use of network or Web access
3311	7.	Illicit content: Storage or distribution of illicit content
3312	8.	Unapproved workaround or shortcut
3313	9.	Unapproved hardware: Use of unapproved hardware or devices
3314	10.	. Unapproved software: Use of unapproved software or services
3315		
3316 3317	Incident Typ modifications. ⁸¹):	bes Involving Physical Actions (based on <u>VERIS</u> with some
3318	1.	Assault (threats or acts of physical violence)
3319	2.	Sabotage (deliberate damaging or disabling)
3320	3.	Snooping (sneak about to gain info or access)
3321	4.	Surveillance (monitoring and observation)
3322	5.	Tampering (alter physical form or function)
3323	6.	Theft (taking assets without permission)
3324	7.	Wiretapping (Physical tap to comms line)
3325		
3326	Incident Typ	es Involving Human (or Technology) Errors (based on
3327	<u>VERIS</u> with some m	nodifications ⁸²):
3328	1.	Classification error (classification or labeling error)
3329	2.	Data entry error
3330	3.	Disposal error
3331	4.	Gaffe (social or verbal slip)
3332	5.	Loss or misplacement
3333	6.	Maintenance error
3334	7.	Misconfiguration
3335	8.	Misdelivery (direct or deliver to wrong recipient)
3336	9.	Omission (something intended, but not done)
3337	10.	. Physical accidents (e.g., drops, bumps, spills)
3338	11.	. Capacity shortage (poor capacity planning)
3339	12.	. Programming error (flaws or bugs in custom code)
3340	13.	. Publishing error (private info to public doc or site)
3341	14.	. Malfunction (technical malfunction or glitch)
3342		

 ⁸¹ <u>Enumerations (verisframework.org)</u>
 ⁸² <u>Enumerations (verisframework.org)</u>

3343	Incident Types Involving Environmental Factors (based on VERIS with
3344	some modifications ⁸³):
3345	1. Deterioration and degradation
3346	2. Earthquake
3347	3. EMI: Electromagnetic interference (EMI)
3348	4. ESD: Electrostatic discharge (ESD)
3349	5. Temperature: Extreme temperature
3350	6. Fire
3351	7. Flood
3352	8. Hazmat: Hazardous material
3353	9. Humidity
3354	10. Hurricane
3355	11. Ice and snow
3356	12. Landslide
3357	13. Lightning
3358	14. Meteorite
3359	15. Particulates: Particulate matter (e.g., dust, smoke)
3360	16. Pathogen
3361	17. Power failure or fluctuation
3362	18. Tornado
3363	19. Tsunami
3364	20. Vermin
3365	21. Volcanic eruption
3366	22. Leak: Water leak
3367	23. Wind
3368	y. Appendix 4: Critical Infrastructure Sectors and
3369	Subsectors
3370	Format of list is as follows:
3371	• Sector
3372	• Subsector
3373	• Chemical

Chemical
Chemical manufacturing or processing plant
Chemical manufacturing or processing plant
Chemical transport
Chemical storage warehousing and storage
Chemical end user
Regulatory, oversight, or industry organization
Commercial facilities

⁸³ Enumerations (verisframework.org)

3380		• Entertainment and media
3381		o Gaming
3382		 Lodging
3383		• Outdoor events
3384		• Public assembly
3385		• Real estate
3386		o Retail
3387		 Sports leagues
3388	٠	Communications
3389		 Information services
3390		 Telecommunications
3391		 Regulatory, oversight, or industry organization
3392	•	Critical Manufacturing
3393		 Primary metal manufacturing
3394		 Machinery manufacturing
3395		• Electrical equipment, appliance, and component manufacturing
3396		 Transportation manufacturing
3397		 Non-critical manufacturing facility
3398	٠	Dams
3399		 Dam project
3400		 Dams control operations facility
3401		 Levees and hurricane barriers
3402		 Navigation locks
3403		 Mine tailing and industrial waste impoundment
3404		 Regulatory, oversight, or industry organization
3405	•	Defense industrial base
3406		 Defense manufacturing facility
3407		 Defense research and development facility
3408		 Defense logistics and asset management facility
3409		 Defense industrial base administration and regulatory facility
3410	•	Emergency services
3411		• Law enforcement
3412		 Fire and emergency services
3413		 Emergency medical services
3414		 Emergency management
3415		 Public works
3416		 Emergency communication
3417	•	Energy
3418		 Electricity
3419		o Petroleum
3420		 Natural gas
3421		o Coal
3422		o Ethanol

3423	0	Biodiesel	
3424	0	Hydrogen	
3425 •	Financ	ial Services	
3426	0	Banking and credit	
3427	0	Securities, commodities, or financial investment	
3428	0	Insurance company	
3429 •	Food a	agriculture	
3430	0	Supply	
3431	0	Processing, packaging, and production	
3432	0	Agriculture and food product storage and distribution warehouse	
3433	0	Agriculture and food product transportation	
3434	0	Agriculture and food product distribution	
3435	0	Agriculture and food supporting facility	
3436	0	Regulatory, oversight, or industry organization	
3437 •	Govern	nment facilities	
3438	0	Elections facilities	
3439	0	K-12 education facilities	
3440	0	Government education facility	
3441	0	Military facility	
3442	0	National monument & icon	
3443	0	Personnel-oriented government facility	
3444	0	Service-oriented government facility	
3445	0	Government sensor or monitoring facility	
3446	0	Government space facility	
3447	0	Government storage or preservation facility	
3448 •	Health	care and public health	
3449	0	Direct patient healthcare	
3450	0	Health information technology	
3451	0	Fatality/mortuary services	
3452	0	Medical materials	
3453	0	Laboratories, blood, and pharmaceuticals	
3454	0	Public health services	
3455	0	Healthcare educational facility	
3456	0	Regulatory, oversight, or industry organization	
3457 •	Inform	nation technology	
3458	0	Hardware production	
3459	0	Software production	
3460	0	Operational support service facility	
3461	0	Internet-based content, information, and communications services	
3462 •	• Nuclear reactors, materials, and waste		
3463	0	Nuclear reactor facility	
3464	0	Nuclear material processing and handling facility	
3465	0	Nuclear waste facility	

3466	Transportation systems
3467	\circ Aviation
3468	• Maritime
3469	 Freight rail
3470	 Highway and motor carrier
3471	 Pipeline
3472	 Postal and shipping
3473	 Mass transit
3474	• Water and wastewater systems
3475	 Drinking water
3476	• Wastewater
3477	• Regulatory, oversight, or industry organization
3478	

3479	z. Appendix 5: Federal Agencies and Sub-Agencies
3480	Format of list is as follows:
3481	• Agency
3482	• Sub-agency
3483	List
3484	Advisory Council on Historic Preservation (ACHP)
3485	African Development Foundation (ADF)
3486	American Battle Monuments Commission (ABMC)
3487	Appalachian Regional Commission (ARC)
3488	Armed Forces Retirement Home
3489	Broadcasting Board of Governors (BBG)
3490	 International Broadcasting Bureau
3491	Central Intelligence Agency (CIA)
3492	Chemical Safety and Hazard Investigation Board (CSHIB)
3493	Commission of Fine Arts (CFA)
3494	Commission on Civil Rights (CCR)
3495	Commodity Futures Trading Commission (CFTC)
3496	Congressional Budget Office
3497	Consumer Financial Protection Bureau (CFPB)
3498	Consumer Product Safety Commission (CPSC)
3499	• Corporation for National and Community Service (CNCS)
3500	 Office of Information Technology
3501	• Court Services and Offender Supervision Agency (CSOSA)
3502	• Defense Nuclear Facilities Safety Board (DNFSB)
3503	• Delaware River Basin Commission (DRBC)
3504	• Department of Agriculture (USDA)
3505	 Agricultural Marketing Service (AMS)
3506	 Agricultural Research Service
3507	 Animal & Plant Health Inspection Service
3508	 Assistant Secretary for Administration
3509	 Assistant Secretary for Congressional Relations
3510	 Chief Financial Officer
3511	 Chief Information Officer (CIO)
3512	 Cooperative State Research, Education, and Extension Service
3513	 Departmental Administration
3514	 Director of Communications
3515	 Economic Research Service
3516	 Executive Operations
3517	 Farm Service Agency
3518	 Food and Nutrition Service

3519	0	Food Safety Inspection Service
3520	0	Foreign Agricultural Service (FAS)
3521	0	Forest Service
3522	0	General Counsel
3523	0	Grain Inspection, Packers and Stockyard Administration
3524	0	Hawaii Agricultural Research Center
3525	0	Information Technology Services (ITS)
3526	0	Inspector General
3527	0	National Agricultural Library
3528	0	National Agriculture Statistics Service
3529	0	National Finance Center (NFC)
3530	0	Natural Resources Conservation Service
3531	0	Office of Communication
3532	0	Office of the Secretary
3533	0	Research, Economics & Education
3534	0	Risk Management
3535	0	Rural Development
3536	0	Telecommunications Services and Operations (TSO)
3537	0	Under Secretary for Farm and Foreign Agricultural Services
3538	0	Under Secretary for Food Nutrition and Consumer Services
3539	0	Under Secretary for Food Safety
3540	0	Under Secretary for Marketing and Regulatory Programs
3541	0	Under Secretary for Natural Resources and Environment
3542	0	Under Secretary for Research Education and Economics
3543	0	Under Secretary for Rural Development
3544 •	Depart	ment of Commerce (DOC)
3545	0	Bureau of Economic Analysis (BEA)
3546	0	Bureau of Export Administration
3547	0	Bureau of Industry and Security
3548	0	Bureau of the Census
3549	0	Chief Information Officer (CIO)
3550	0	DOC-CIRT
3551	0	Economic Development Administration
3552	0	Economics and Statistics Administration
3553	0	FEDWorld
3554	0	International Trade Administration (ITA)
3555	0	Minority Business Development Agency
3556	0	National Institute of Standards & Technology (NIST)
3557	0	National Marine Fisheries Service (NMFS)
3558	0	National Ocean Service
3559	0	National Oceanic & Atmospheric Administration (NOAA)
3560	0	National Technical Information Service (NTIS)
3561	0	National Telecommunications & Information Administration
3562	0	National Weather Service
--------	--------	--
3563	0	Office of Inspector General
3564	0	Office of the Secretary
3565	0	Patent and Trademark Office
3566	0	Technology Administration
3567	0	U.S. Patent and Trademark Office
3568 •	Depart	ment of Defense (DOD)
3569	0	Air Force (USAF)
3570	0	American Forces Press Service
3571	0	Army (USA)
3572	0	Chief Information Officer (CIO)
3573	0	Defense Commissary Agency
3574	0	Defense Contract and Audit Agency (DCAA)
3575	0	Defense Finance and Accounting Service (DFAS)
3576	0	Defense Information Systems Agency (DISA)
3577	0	Defense Intelligence Agency (DIA)
3578	0	Defense Logistics Agency (DLA)
3579	0	Defense Security Service
3580	0	Defense Technical Information Center (DTIC)
3581	0	Joint Chiefs of Staff (JCS)
3582	0	Joint Task Force-Global Network Operations (JTF-GNO)
3583	0	Marine Corps (USMC)
3584	0	Missile Defense Agency (MDA)
3585	0	National Guard
3586	0	National Security Agency (NSA)
3587	0	Navy (USN)
3588 •	Depart	ment of Education (EDUC)
3589	0	Chief Information Officer (CIO)
3590	0	Educational Resources Information Center (ERIC)
3591	0	Federal Student Aid (FSA)
3592	0	National Library of Education (NLE)
3593	0	Office of Educational Technology
3594	0	Office of General Counsel
3595	0	Office of Inspector General
3596	0	Office of Intergovernmental and Interagency Affairs
3597	0	Office of Legislation and Congressional Affairs
3598	0	Office of Management
3599	0	Office of Public Affairs
3600	0	Office of the Chief Financial Officer
3601	0	Office of the Chief Information Officer
3602	0	Office of the Secretary
3603 •	Depart	ment of Energy (DOE)
3604	0	Ames Laboratory

3605	0	Argonne National Laboratory (ANL)
3606	0	Assistant Secretary for Congressional and Intergovernmental
3607	0	Assistant Secretary for Environment Safety and Health (ES&H)
3608	0	Assistant Secretary for Environmental Management
3609	0	Assistant Secretary for Fossil Energy
3610	0	Assistant Secretary for Policy and International Affairs
3611	0	Associate Administrator for Facilities and Operations
3612	0	Associate Administrator for Management and Administration
3613	0	Brookhaven National Lab
3614	0	Chief Information Officer (CIO)
3615	0	Computer Incident Advisory Capability (CIAC)
3616	0	Defense Nuclear Facilities Safety Board Liaison
3617	0	Deputy Administrator for Defense Nuclear Nonproliferation
3618	0	Deputy Administrator for Defense Programs
3619	0	Deputy Administrator for Naval Reactors
3620	0	Energy Information Administration
3621	0	Federal Energy Regulatory Commission
3622	0	FermiLab
3623	0	General Counsel
3624	0	Idaho National Labs
3625	0	Lawrence Berkeley National Laboratory
3626	0	Lawrence Livermore National Laboratory
3627	0	Los Alamos National Laboratory
3628	0	Oak Ridge National Labs
3629	0	Office of Civilian Radioactive Waste Management
3630	0	Office of Counterintelligence
3631	0	Office of Economic Impact and Diversity
3632	0	Office of Emergency Operations
3633	0	Office of Hearings and Appeals
3634	0	Office of Independent Oversights and Performance Assurance
3635	0	Office of Intelligence
3636	0	Office of Management Budget and Evaluation/Chief Financial
3637	0	Office of Nuclear Energy Science and Technology
3638	0	Office of Public Affairs
3639	0	Office of Science
3640	0	Office of Security
3641	0	Office of the Inspector General
3642	0	Office of the Secretary
3643	0	Office of Worker and Community Transition
3644	0	Power Marketing Administrations
3645	0	Secretary of Energy Advisory Board
3646	0	Southwestern Power Administration
3647	0	Under Secretary for Energy Science and Environment

3648	0	Under Secretary for Nuclear Security
3649 •	Depart	tment of Health and Human Services (HHS)
3650	0	Administration for Children and Families
3651	0	Administration on Aging
3652	0	Agency for Healthcare Research and Quality (AHCRQ)
3653	0	Agency for Toxic Substances and Disease Registry
3654	0	Centers for Disease Control and Prevention (CDC)
3655	0	Centers for Medicare and Medicaid Services (CMS)
3656	0	Chief Information Officer (CIO)
3657	0	Financial Management Systems
3658	0	Food and Drug Administration (FDA)
3659	0	Health Resources and Services Administration
3660	0	Indian Health Service
3661	0	National Institutes of Health (NIH)
3662	0	Office of Inspector General
3663	0	Office of the Secretary
3664	0	Program Support Center
3665	0	Secure One Communications Center (SOCC)
3666	0	Substance Abuse and Mental Health Services Administration
3667 •	Depart	tment of Homeland Security (DHS)
3668	0	Bureau of Citizenship and Immigration Services
3669	0	Chief Information Officer (CIO)
3670	0	Cybersecurity and Infrastructure Security Agency (CISA)
3671	0	CSIRC
3672	0	Customs & Border Protection
3673	0	Federal Emergency Management Agency (FEMA)
3674	0	Federal Law Enforcement Training Center
3675	0	Federal Protective Service (FPS)
3676	0	Headquarters
3677	0	HSOC
3678	0	Immigration and Customs Enforcement (ICE)
3679	0	Information Analysis Infrastructure Protection (IAIP)
3680	0	National Coordinating Center (NCC Watch)
3681	0	National Infrastructure Coordination Center (NICC)
3682	0	NCSD
3683	0	Office of Immigration Statistics
3684	0	Office of the Inspector General (OIG)
3685	0	Science and Technology Directorate
3686	0	Iransportation Security Administration (TSA)
3687	0	United States Coast Guard
3688	0	United States Secret Service
3689 •	Depart	tment of Housing and Urban Development (HUD)
3690	0	Administration

3691	0	Chief Financial Officer
3692	0	Chief Information Officer (CIO)
3693	0	Chief Procurement Officer
3694	0	Community Planning and Development
3695	0	Congressional and Intergovernmental Relations
3696	0	Enforcement Center
3697	0	Federal Housing Enterprise Oversight
3698	0	General Counsel
3699	0	Government National Mortgage Association (Ginnie Mae)
3700	0	Housing and Urban Development Reading Room
3701	0	Inspector General
3702	0	Multifamily Housing Assistance Restructuring
3703	0	Office of Departmental Equal Employment Opportunity
3704	0	Office of Departmental Operations and Coordination
3705	0	Office of Healthy Homes and Lead Hazard Control
3706	0	Office of the Secretary
3707	0	Policy Development and Research
3708	0	Public Affairs
3709	0	Public and Indian Housing
3710	0	Real Estate Assessment Center
3711	• Depart	ment of Justice (DOJ)
3712	0	Antitrust Division (ATR)
3713	0	Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
3714	0	Civil Division
3715	0	Civil Rights Division
3716	0	Community Relations Service
3717	0	Criminal Division
3718	0	DOJCERT
3719	0	Drug Enforcement Agency (DEA)
3720	0	Environment and Natural Resources Division
3721	0	Executive Office for Immigration Review
3722	0	Executive Office for the U.S. Attorneys
3723	0	Executive Office for the U.S. Trustees
3724	0	Federal Bureau of Investigation (FBI)
3725	0	Federal Bureau of Prisons
3726	0	Inspector General
3727	0	Intelligence Policy and Review
3728	0	Intergovernmental Affairs
3729	0	Justice and Management Division
3730	0	Legal Counsel
3731	0	Legal Policy
3732	0	Legislative Affairs
3733	0	National Drug Intelligence Center (NDIC)

3734		0	Office of Community Oriented Policing Services
3735		0	Office of Federal Detention Trustee (OFDT)
3736		0	Office of Information & Privacy (OIP)
3737		0	Office of Justice Programs (OJP)
3738		0	Office of Professional Responsibility (OPR)
3739		0	Office of the Associate Attorney General
3740		0	Office of the Attorney General
3741		0	Office of the Deputy Attorney General
3742		0	Office of the Pardon Attorney
3743		0	Office of the Solicitor General
3744		0	Public Affairs
3745		0	Tax Division
3746		0	U.S. National Central Bureau - INTERPOL (USNCB)
3747		0	U.S. Parole Commission
3748		0	U.S. Trustee Program (USTP)
3749		0	United States Marshals Service (USMS)
3750	•	Depart	tment of Labor (DOL)
3751		0	Administration Review Boards (ARB)
3752		0	Benefits Review Board (BRB)
3753		0	Bureau of International Labor Affairs (ILAB)
3754		0	Bureau of Labor Statistics (BLS)
3755		0	Center for Faith-Based and Community Initiatives
3756		0	Employee Benefit Securities Administrations (EBSA)
3757		0	Employee's Compensation Appeals Board (ECAB)
3758		0	Employment Standards Administration (ESA)
3759		0	Employment Training Administration (ETA)
3760		0	Mine Safety Health Administration (MSHA)
3761		0	National Mine Health and Safety Academy
3762		0	Office of Congressional and Intergovernmental Affairs
3763		0	Office of Disability Employment Policy (ODEP)
3764		0	Office of Job Corps (OJC)
3765		0	Office of Public Affairs (OPA)
3766		0	Office of Safety and Health Administration (OSHA)
3767		0	Office of Small Business Programs (OSBP)
3768		0	Office of the Administrative Law Justices (ALJ)
3769		0	Office of the Assistant Secretary for Policy (OASP)
3770		0	Office of the Chief Financial Officer (OCFO)
3771		0	Office of the Inspector General (OIG)
3772		0	Office of the Secretary (OSEC)
3773		0	Office of the Solicitor of Labor (SOL)
3774		0	Veterans Employment and Training Service (VETS)
3775		0	Women's Bureau (WB)
3776	•	Depart	tment of State (DOS)

3777	0	Agricultural Economics and Business Affairs		
3778	0	Appellate Review Board		
3779	0	Board of the Foreign Service		
3780	0	Bureau of Diplomatic Security		
3781	0	Chief Information Officer (CIO)		
3782	0	Commissions		
3783	0	Coordinator for Counterterrorism		
3784	0	Counselor of the Department		
3785	0	Country Officers		
3786	0	Democracy Human Rights and Labor Bureau		
3787	0	Department of State Library		
3788	0	Deputy Secretary		
3789	0	Examiners for the Foreign Service		
3790	0	Executive Secretariat		
3791	0	Foreign Service Grievance Board		
3792	0	Historian		
3793	0	Intelligence and Research		
3794	0	Legal Adviser		
3795	0	Legislative Affairs		
3796	0	NATO (North Atlantic Treaty Organization)		
3797	0	Office of the Secretary		
3798	0	Office of the United Nations Ambassador		
3799	0	Policy Planning Staff		
3800	0	Under Secretary for Arms Control and International Security		
3801	0	Under Secretary for Global Affairs		
3802	0	Under Secretary for Management		
3803	0	Under Secretary for Political Affairs		
3804	0	Under Secretary for Public Diplomacy and Public Affairs		
3805	0	United National Political Affairs		
3806	• Department of the Interior (DOI)			
3807	0	Bureau of Indian Affairs		
3808	0	Bureau of Land Management		
3809	0	Bureau of Reclamation		
3810	0	Chief Information Officer (CIO)		
3811	0	DOI CIRC		
3812	0	Fish and Wildlife Service		
3813	0	Minerals Management Service		
3814	0	National Business Center		
3815	0	National Park Service		
3816	0	Office of Hearings and Appeals		
3817	0	Office of Surface Mining		
3818	0	Office of the Inspector General		
3819	0	Office of the Secretary		

3820		0	US Geological Survey
3821	•	Depart	tment of the Treasury
3822		0	Alcohol and Tobacco Tax and Trade Bureau (TTB)
3823		0	Bureau of Alcohol Tobacco and Firearms (ATF)
3824		0	Bureau of Engraving and Printing
3825		0	Bureau of the Fiscal Service (BFS)
3826		0	Chief Information Officer (CIO)
3827		0	Comptroller of the Currency
3828		0	Executive Office for Asset Forfeiture
3829		0	Federal Law Enforcement Training Center
3830		0	Financial Crimes Enforcement Network
3831		0	Internal Revenue Service (IRS)
3832		0	Office of the Comptroller of the Currency
3833		0	Office of the Inspector General
3834		0	Office of the Secretary
3835		0	Office of Thrift Supervision (OTS)
3836		0	TCSIRC
3837		0	Treasury Headquarters (Treas-HQ)
3838		0	United States Customs Services
3839		0	United States Mint
3840		0	US Federal Civilian Agency
3841	•	Depart	tment of Transportation (DOT)
3842		0	Bureau of Transportation Statistics
3843		0	Chief Information Officer (CIO)
3844		0	Federal Aviation Administration (FAA)
3845		0	Federal Highway Administration
3846		0	Federal Motor Carrier Safety Administration
3847		0	Federal Railroad Administration
3848		0	Federal Transit Administration
3849		0	Maritime Administration
3850		0	National Highway Traffic Safety Administration
3851		0	Office of the Inspector General
3852		0	Office of the Secretary
3853		0	Research and Special Programs Administration
3854		0	Saint Lawrence Seaway Development Corporation
3855		0	Surface Transportation Board
3856		0	Transportation Administrative Services Center
3857		0	Transportation CIRC (TCIRC)
3858	•	Depart	tment of Veterans Affairs
3859		0	Acquisition and Material Management
3860		0	Acute Care Strategic Healthcare Group
3861		0	Administration and Human Resources
3862		0	Allied Clinical Services Strategic Healthcare Group

3863	0	Audit
3864	0	Austin Automation Center
3865	0	Board of Contract Appeals
3866	0	Board of Veterans' Appeals
3867	0	Budget
3868	0	Chief Information Officer (CIO)
3869	0	Congressional and Legislative Affairs
3870	0	Deputy Secretary
3871	0	Disadvantaged and Small Business Utilization
3872	0	Diversity Management and Equal Employment Opportunity
3873	0	Emergency Management Strategic Healthcare Group
3874	0	Employee Education
3875	0	Facilities Management
3876	0	Facilities Service
3877	0	General Counsel
3878	0	Geriatrics and Extended Care Strategic Healthcare Group
3879	0	Information and Technology
3880	0	Inspector General
3881	0	Intergovernmental and Public Affairs
3882	0	Law Enforcement and Security
3883	0	Litigation Docket
3884	0	Management
3885	0	National Cemetery Administration
3886	0	Nursing Strategic Healthcare Group
3887	0	Office of Dentistry
3888	0	Office of Investigations
3889	0	Office of the Secretary
3890	0	Patient Care Services
3891	0	Planning and Elution
3892	0	Planning and Policy
3893	0	Policy Office
3894	0	Primary and Ambulatory Care Strategic Healthcare Group
3895	0	Quality and Performance Office
3896	0	Readjustment Counseling Service
3897	0	Rehabilitation Strategic Healthcare Group
3898	0	Research and Development
3899	0	Support Service
3900	0	Telecommunications
3901	0	VACIRC
3902	0	VASOC
3903	0	Veterans Benefits Administration
3904	0	Veterans Health Administration
3905 •	Enviro	nmental Protection Agency (EPA)

3906	٠	Equal Employment Opportunity Commission (EEOC)
3907	٠	Executive Office of the President (EOP)
3908		 Office of Management and Budget (OMB)
3909		 United States Trade Representative (USTR)
3910		• White House
3911	٠	Export-Import Bank of the United States (EIIM)
3912	•	Fannie Mae (FNMA)
3913	•	Farm Credit Administration (FCA)
3914	٠	Federal Accounting Standards Advisory Board (FASAB)
3915	•	Federal Communications Commission (FCC)
3916	•	Federal Deposit Insurance Corporation (FDIC)
3917	•	Federal Election Commission (FEC)
3918	•	Federal Energy Regulatory Commission (FERC)
3919	•	Federal Housing Finance Agency (FHFA)
3920	٠	Federal Judiciary
3921		 Administrative Office of the United States Courts
3922	٠	Federal Labor Relations Authority (FLRA)
3923	٠	Federal Maritime Commission (FMC)
3924	٠	Federal Mediation and Conciliation Service (FMCS)
3925	•	Federal Mine Safety and Health Review Commission (FMSHRC)
3926	•	Federal Reserve System (FRS)
3927		 Board of Governors
3928	•	Federal Retirement Thrift Investment Board (FRTIB)
3929		 Thrift Savings Plan
3930	•	Federal Trade Commission (FTC)
3931	•	Freddie Mac (FHLMC)
3932	•	General Services Administration (GSA)
3933	٠	Government Printing Office
3934	•	Harry S Truman Scholarship Foundation (HTSF)
3935	٠	Holocaust Memorial Council (HMC)
3936	٠	House of Representatives
3937	٠	Independent Agencies
3938		 United States Consumer Product Safety Commission (CPSC)
3939	٠	Institute of Museum and Library Services (IMLS)
3940	٠	Institute of Peace United States (USIP)
3941	•	Inter-American Foundation (IAF)
3942	•	International Boundary and Water Commission
3943	٠	International Broadcasting Bureau (IBB)
3944	•	International Trade Commission (ITC)
3945	٠	ISAC
3946		 Airport

3947	• Chemical
3948	 Electricity
3949	 Emergency Fire Services
3950	 Energy
3951	 Financial Services (FS)
3952	 Food and Agriculture
3953	 Information Technology (IT)
3954	• Maritime
3955	• Multi-State (MS)
3956	 National Monuments and Icons
3957	 Postal and Shipping
3958	• Public Health
3959	• Real Estate
3960	 Research and Education
3961	• State CIO
3962	 Surface Transportation
3963	o Telecom
3964	• Trucking
3965	• Water
3966 •	James Madison Memorial Fellowship Foundation (JMMFF)
3967 •	Japan - United States Friendship Commission (JUSFC)
3968 •	Javits-Wagner-O'Day Program (JWOD)
3969 •	Legal Services Command (LSC)
3970 •	Library of Congress
3971 •	Marine Mammal Commission (MMC)
3972 •	Merit Systems Protection Board (MSPB)
3973 •	Millennium Challenge Corporation (MCC)
3974 •	National Aeronautics and Space Administration (NASA)
3975	• Ames Research Center (ARC)
3976	• Chief Information Officer (CIO)
3977	• Glenn Research Center (GRC)
3978	 Goddard Space Flight Center (GSFC)
3979	 Jet Propulsion Laboratories (JPL)
3980	 Johnson Space Center (JSC)
3981	 Kennedy Space Flight Center (KSFC)
3982	 Langley Research Center (LRC)
3983	 Marshall Space Flight Center (MSFC)
3984	• NASIRC
3985	 Stennis Space Center
3986	 Wallops Flight Facility (WFF)
3987 •	National Archives and Records Administration (NARA)
3988 •	National Capital Planning Commission (NCPC)

3989	٠	National Council on Disability (NCD)
3990	٠	National Credit Union Administration (NCUA)
3991	•	National Endowment for the Arts
3992	٠	National Endowment for the Humanities
3993	٠	National Foundation on the Arts and the Humanities (NFAH)
3994	٠	National Gallery of Arts (NGA)
3995	٠	National Indian Gaming Commission (NIGC)
3996	٠	National Institute for Literacy
3997	٠	National Labor Relations Board (NLRB)
3998	٠	National Mediation Board (NMB)
3999	٠	National Railroad Passenger Corporation (AMTRAK)
4000	٠	National Science Foundation (NSF)
4001		 US Climate Change Science Program (USGCRP)
4002	٠	National Transportation Safety Board (NTSB)
4003	٠	Neighborhood Reinvestment Corporation (NBRC)
4004	٠	Nuclear Regulatory Commission (NRC)
4005	٠	Nuclear Waste Technical Review Board United States (NWTRB)
4006	•	Occupational Safety and Health Administration (OSHA)
4007	٠	Occupational Safety and Health Review Commission (OSHRC)
4008	٠	Office of Federal Housing Enterprise Oversight (OFHEO)
4009	٠	Office of Government Ethics (OGE)
4010	٠	Office of Navajo & Hopi Indian Relocation
4011	٠	Office of Personnel Management
4012	٠	Office of Special Counsel (OSC)
4013	٠	Office of the Director of National Intelligence (ODNI)
4014		 Information Sharing Environment (ISE)
4015		 Intelligence Advanced Research Projects Activity (IARPA)
4016		 National Counterproliferation Center (NCPC)
4017		 National Counterterrorism Center (NCTC)
4018		 National Intelligence Council (NIC)
4019		 Office of the National Counterintelligence Executive (ONCIX)
4020	•	Open Source Information System (OSIS)
4021	٠	Peace Corps (PC)
4022	٠	Pension Benefit Guaranty Corporation (PBGC)
4023	٠	Postal Rate Commission (PRC)
4024	٠	Railroad Retirement Board (RRB)
4025	•	Recovery Accountability and Transparency Board
4026	٠	Securities and Exchange Commission (SEC)
4027	٠	Selective Service System (SSS)
4028	٠	Small Business Administration (SBA)
4029	٠	Smithsonian Institute (SI)

Social Security Administration (SSA) 4030 State Justice Institute (SJI) 4031 Susquehanna River Basin Commission (SRBC) 4032 • Tennessee Valley Authority (TVA) 4033 • U.S. International Development Finance Corporation (DFC) 4034 • U.S. Senate 4035 • • U.S. Trade and Development Agency (TDA) 4036 United States Agency for International Development (USAID) 4037 • 4038 • United States Arms Control and Disarmament Agency (ACDA) United States Congress 4039 • • Government Accountability Office (GAO) 4040 United States International Trade Commission (USITC) 4041 • United States Postal Service (USPS) 4042 • 4043 • United States Trade and Development Agency US-China Economic and Security Review Commission (USCC) 4044 • Voice of America (VOA) 4045 • 4046

Privacy Act Statement

Incident Reporting Form 2.0

Authority: 44 U.S.C. § 3101 & 3556, and 6 U.S.C. § 659(c)(1), (3), (9) authorize the collection of this information.

Purpose: The primary purpose for the collection of this information is to allow the Cybersecurity and Infrastructure Security Agency (CISA) to contact you about your request.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

Disclosure: Some entities are regulatorily or statutorily required to submit incident reports to CISA, and those entities must provide information in this form as required by applicable statute, regulation, or similar mandate. Failure to provide this information may result in inaccurate record keeping of the entity's compliance. For non-mandatory incident reporting, providing this information is voluntary. However, failure to provide this information will prevent CISA from contacting you in the event there are questions about your report.

Paperwork Burden Notice:

The public reporting burden to complete this information collection is estimated at 60 minutes per form response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. 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 OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/ CISA/CSD, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [OMB Control No. 1670-00XX].