1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	<b>CISA Incident Reporting Form</b>
	Complete Question Set
15	<b>Complete Question Set</b>
15 16	Complete Question Set
	Complete Question Set
16	Complete Question Set
16 17	Complete Question Set
16 17 18	Complete Question Set
16 17 18 19	Complete Question Set
16 17 18 19 20	Complete Question Set
16 17 18 19 20 21	Complete Question Set
116 117 118 119 220 221 222 223	Complete Question Set
116 117 118 119 220 221 222 223 224	Complete Question Set
116 117 118 119 220 221 222 223 224 225	Complete Question Set
116 117 118 119 220 221 222 223 224	Complete Question Set

Ta	ble	of	Con	iten	ts

29 30

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:	<u>c</u>
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	30
43	Confidentiality, Integrity, Availability (CIA) Assessment	30
44	Violation of Law and Policy	31
45	Incident: High-Level Impacts	31
46	Public Impacts	31
47	National US Impacts	31
48	Regional Impacts (Local to Global)	
49	Breach Severity Impacts	32
50	Major Incident Severity Determination (FISMA Only)	33
51	Public Health and Safety Impacts	34
52	Indirect Impacts	35
53	Impacts Internal to the Entity	37
54	Functional Impacts to Entity	37
55	Informational Impacts to Entity	38
56	Physical Impacts to Entity	39
57	Economic Impacts to Entity	39
58	k. Incident Details	40
59	Incident: Details by Stage	40
60	1. Identification and Detection (I/D) Stage	40
61	Incident Stage (I/D): Pansamware and Cuber Extertion	40

62	Initial Ransom Demand Details	40
63	Ransom Payment Details	41
64	Results of Ransom Incident	46
65 66	Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) and Indicators of Compromise (I-D) Observed	
67	Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) Observed	47
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	
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	
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 Reference	es91
104	Protect CISA CPGs & NIST SP 800-53 References	
105	x. Appendix 3: Incident Type/Categories	
106	Incident Types involving Malware	
107	Incident Types Involving Hacking	100
108	Incident Types Involving Social Engineering	
109	Incident Types Involving Misuse of Assets	
110	Incident Types Involving Physical Actions	
111	Incident Types Involving Human (or Technology) Errors	
112	Incident Types Involving Environmental Factors	
113	y. Appendix 4: Critical Infrastructure Sectors and Subsectors	
114	z. Appendix 5: Federal Agencies and Sub-Agencies	107
115		
116		
117		
118		
119		
120		
121		
122		
123		
124		
125		
126		
127		

128	a. Introduction
129 130	The Cybersecurity and Infrastructure Security Agency (CISA) collects cybersecurity incident 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
132	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
134	distinct from incident reporting under the Cyber Incident Reporting for Critical Infrastructure
135 136	Act (CIRCIA). CISA will use a different information collection instrument for CIRCIA incident 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
140 141	Portal respondents will be directed to answer a subset of the questions based on the characteristics 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
143	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
145	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
149 150	impact the flow from question-to-question, to indicate where certain respondents may be able to indicate they would like certain data markings applied to their responses to the question, and to
151	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	[RR] = Required question for reports identified as necessary to satisfy a regulatory and/or
156	statutory requirement including Federal Information Security Modernization Act
157	(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:
176 177 178	Display notes do not contain questions with which a respondent must engage. Display notes contain additional explanatory content which may assist a respondent with 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.
183 184 185 186 187 188 189 190	Design notes are intended to enable the developers of the Incident Reporting Portal and reviewers of the question understand the conditional logic which may direct a respondent from one question to the appropriate next question based on their input. The flow from question-to-question will continue to be under development as CISA incorporates feedback from reviewers. However, since it is critical to communicate that no respondent will answer all the questions contained herein, we wanted to provide this conditional logic to support reviewers' understanding of how the dynamic form may work. The 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.)
193 194	c. Beginning of Incident Reporting Questions
195 196	(DISPLAY NOTE: Global Disclaimer: Please fill out all questions in this form to the best of your knowledge at the time of submission.)
197 198	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. <sup>1</sup>
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 <sup>2</sup> , 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
221 222	of compliance, you must indicate the specific requirement below to be considered as reporting under that requirement.)
223	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
230	ej seiseculty metacht
231	B. Federal Energy Regulatory Commission (FERC)/ North American Electric
232	Reliability Corporation (NERC)
	remaining Corporation (Table)

<sup>1</sup> **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.

<sup>&</sup>lt;sup>2</sup> 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	(66 1.1. 1.2. 1.6. 1.6. 1.1. 1.1. 1.1. 1.
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)
	1. (DESIGNATOLE, TOPORTICASUM 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
	2. Alternate
286	
287	C. [CUI] Email address(es)  1. Preferred
288	
289	2. Alternate
290	D. [CUI] Social media profile (Optional)
291	1. Primary social media handle or username?
292	2. Enter the corresponding social media platform
293	E. Job title
294	F. Which time zone are you in?
295	
296	5. [CUI][RA] Are you the primary point of contact for this incident? (Yes/No)
297	A. [CUI][RC] (DESIGN NOTE: If No) Please provide the primary point of contact name
298	and contact information
299	1. [CUI]Name
300	a. First
301	b. Last
302	2. [CUI]Phone number(s)
303	a. Preferred
304	b. Alternate
305	3. [CUI]Email address(es) of point of contact
306	a. Preferred
307	b. Alternate
308	4. [CUI] Social media profile (Optional)
309	a. Primary social media handle or username?
310	b. Enter the corresponding social media platform
311	5. Job title
312	6. 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
331 332	requirement >> DISPLAY NOTE: If a third party is submitting a report on behalf of the impacted 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
334	requirement must allow for third-party submission of reports. CISA will not verify whether third-
335 336	party submission of a report fully satisfies other legal reporting requirements on behalf of an impacted
337	entity.)  1. [CUI]Please 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
	1. First
340	
341	2. Last
342	b. [CUI]Phone 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 <b><u>not</u></b> have the consent and/or have <b><u>not</u></b> 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
352 353	without consent and/or authorization, this incident will be validated between the impacted entity and

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 <sup>3</sup> ? (Yes/No)
372	1. {Conditional to "Voluntary" report AND "Yes" to "operating a critical
373	infrastructure" 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
375 376	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 <sup>4</sup> , 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.
JJ2	officed States, of tiffeatens public fleatin of safety.

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
 PCII Program - Frequently Asked Questions | CISA (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,
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 PCII protections to be afforded to you
407	for this report you will need to complete and return the "Express and Consent"
408	statement that CISA will send to you via the email contact information you provided
409 410	in this form. (DISPLAY NOTE: To learn more about the benefits the PCII program affords qualified submissions please visit, https://www.cisa.gov/resources-
411	tools/programs/protected-critical-infrastructure-information-pcii-programs/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
	l. Healthcare and Public Health
433	
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 <sup>7</sup> 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
460 461	Gov entities as "Government facilities" for prime critical infrastructure sector, then allow for one-to-
462	many secondary critical infrastructure sectors and sub sectors)  1. Chemical
463	2. Commercial Facilities
464	3. Communications
465	4. Critical Manufacturing
	5. Dams
466 467	
467 460	
468	7. Emergency Services
469	8. Energy
470	9. Financial Services
471	10. Food and Agriculture
472	11. Government Facilities

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

<sup>&</sup>lt;sup>6</sup> 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. [RC] (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 SLTT options: (DESIGN NOTE: Single select)
492	1. [] 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).8
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)
504 505	2. Please select the associated state or territory below (DESIGN
505 506	NOTE: Select from list) <sup>9</sup> 3. [ ] Tribal
507 508	•
508	name and any U.S. states and/or territories where the tribe is
509	physically located.

<sup>&</sup>lt;sup>8</sup> 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
515 516	one entry as a tribe maybe physically spread across several states and
517	regions)  B. Is the impacted SLTT Entity in a critical infrastructure sector? 11 (Yes/No)
518	1. {Conditional to "voluntary" report AND "Yes" to "operating a critical
519	infrastructure" AND "entity type" is not "Federal Government" (DESIGN
520	NOTE: If this is flagged as a "voluntary" report and "Yes" as operating a critical infrastructure
521	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 <sup>12</sup> , 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,

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

<sup>11</sup> https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
12 PCII Program - Frequently Asked Questions | CISA (https://www.cisa.gov/resources-tools/programs/protected-critical-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
555 556	afforded to you for this report. (DISPLAY NOTE: To learn more about the benefits
557	the PCII program affords qualified submissions please visit, "https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-
558	information-pcii-program/pcii-program-frequently-asked-questions".))
559	1. If you do not wish to have your submission evaluated as a
560	PCII submission, please check this box []
561	c. (DESIGN NOTE: If No: (DISPLAY NOTE: Thank you. Your submission does not
562	seem to meet the conditions to qualify as protected critical infrastructure
563	information. You may now continue with the rest of the form.)
564	2. (DESIGN NOTE: If Yes) Please select the primary critical infrastructure sector
565	that is impacted by this incident. If applicable, also select the appropriate
566	critical infrastructure-subsector. (DESIGN NOTE: See Appendix 4 for complete critical
567	infrastructure Sector and subsector list. Primary critical infrastructure Sector can only be
568	entered once.)
569	1. Chemical
570	2. Commercial Facilities
571	3. Communications
572	4. Critical Manufacturing
573	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 <sup>14</sup> (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.)  1. Chemical
609	
610	<ul><li>2. Commercial Facilities</li><li>3. Communications</li></ul>
611	
612	<ul><li>4. Critical Manufacturing</li><li>5. Dams</li></ul>
613	
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 (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)

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). <sup>16</sup>
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	subsector list. Primary critical infrastructure sector can only be entered once.)
651 652	(DESIGN NOTE: Flag all Federal Gov entities as "government facilities" as their 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
	12. Healthcare and Public Health
665	
666	13. Information Technology
667	14. Nuclear Reactors, Materials, and Waste

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

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-
679 680	subsector. (DESIGN NOTE: See Appendix 4 for complete critical infrastructure 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	to the primary contract impacted by or involved in this incident. (DESIGN NOTE:
684	Allow one to many entries) (DESIGN NOTE: Allow "button" to add to the contract list if necessary
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 No) 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
722	Government Administrative Contracting Officer (ACO). <sup>17</sup> and US Government Program
723	Manager (PM).) (DESIGN NOTE: Allow for more than one entry)
724	a. Name
725	1. First
726	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
730 731	"dropdown list" to select from example list, allow "OTHER" with a fill-in description)
732	e. Address
733	1. Street name and number
734	2. Postal code
735	3. City
736	4. State
737	5. Country
738	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
,	11. The provide details about the impacted of the boolety entity

<sup>17</sup> 48 CFR § 842.271 - Administrative Contracting Officer's role in contract administration and delegated functions. <u>Electronic Code of Federal Regulations (e-CFR) | US Law | LII / Legal Information Institute (cornell.edu</u>

<sup>18</sup> 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
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777

778

779

- 1. Please describe your organization's sector within civil society (e.g., academia, faith-based, think tank, media, advocacy, political party, labor union) (DESIGN NOTE: Open text)
- 2. Please enter the civil society entity's name (spell out any acronyms)
- B. Are there any critical infrastructure (critical infrastructure) sector(s). <sup>19</sup> directly impacted by the incident that occurred/is occurring at your organization? (Yes/No)
  - 1. {Conditional to "voluntary" report AND "Yes" to "operating a critical infrastructure" AND "entity type" is not "Federal Government"} (DESIGN 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 PCII conditions must be met and asked of the reporter) You have indicated your entity directly impacts a critical infrastructure sector and is also submitting this report on a voluntary basis. So that your report can be evaluated for protections afforded under the Protected Critical Infrastructure Information (PCII) Program <sup>20</sup>, do you consider the information you are sharing to meet any of the following conditions? Select "Yes" if any of the following conditions are true. (Yes/No)
    - a. Is the information, not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, communication networks, or other information concerning:
      - 1. Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, State, local, tribal, territorial laws, harms interstate commerce of the United States, or threatens public health or safety.
      - 2. The ability of any critical infrastructure or protected system to prevent such interference, compromise, or incapacitation; including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
      - 3. Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the

<sup>&</sup>lt;sup>19</sup> https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

<sup>&</sup>lt;sup>20</sup> <u>PCII Program - Frequently Asked Questions | CISA (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)</u>

780	extent it is related to such interference, compromise, or
781	incapacitation.
782 783 784 785 786 787 788 789 790 791	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.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions".))  1. If you do not wish to have your submission evaluated as a 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 Yes) 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
835 836	should be entered. both could be allowed, but at least one location designation should be required)
837	3. Street name and number
838	
	<ul><li>4. City</li><li>5. State</li></ul>
839	
840	6. Postal code
841	7. Country. <sup>21</sup>
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
845 846	towers in the communications sector or offshore oil platforms in the oil and natural gas (ONG) subsector, do not have street addresses. Understanding the geographic location can help CISA identify
847	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)? (Yes/No)
855	1. (DESIGN NOTE: If Yes) Please describe the entity that was involved in this
856	incident. (DESIGN NOTE: Open text)
857	18. [Op] + [RR] Please provide the following information about the impacted
858	organization. (Answer for the impacted entity and not the parent entity.)
	A. Do you know if the impacted entity that owns and/or operates the facility(ies)
859 860	
860	where the incident occurred has any unique government or business
861	identifiers (e.g. North American Industrial Classification System (NAICS),

<sup>&</sup>lt;sup>21</sup> 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
880 881	codes provide a standardized method of identifying a given facility at a specific location.)
882	1. Street name and number
883	2. Building number (if applicable)
884	3. Suite number (if applicable)
885	4. City
886	5. State
887	6. Postal code
888	7. Country. <sup>22</sup>
889	5. Other [please provide the type of identifier]
890	3. Other [piease provide the type of identifier]
891	19. [RC] (DESIGN Note: applies only to "Third Party" selection in "red box")
551	[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)

 $<sup>^{22}</sup>$  Use CISA data standards where applicable (<u>Office of the Chief Information Officer - Active Data Standards - All 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
917 918	summary" of the incident with a narrative of the incident detection. Consider including a description of any
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
931 932	incident (DESIGN NOTE: Multi select, then drop down for more refined selections within each main 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,
934 935	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 <sup>23</sup> )
954	H. Operational technology process control impaired (e.g., physical control processes
955	are manipulated, disabled, or damaged. <sup>24</sup> )
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
960	customer)
961	K. Unauthorized account access
962	L. Unauthorized removal of account access (e.g., entity's system administrator's
963	account deleted)
964	M. Unauthorized information access
965	N. Unauthorized release of information (virtually via computing systems). <sup>25</sup>

<sup>23</sup> Inhibit Response Function, Tactic TA0107 - ICS | MITRE ATT&CK®

<sup>25</sup> Unauthorized release of information "virtually" is an occurrence where a person other than an authorized user

<sup>&</sup>lt;sup>24</sup> Impair Process Control, Tactic TA0106 - ICS | MITRE ATT&CK®

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). <sup>26</sup>
968	P. Unauthorized use of information
969	Q. Other [describe]
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
974 975	reporting obligations on your or your organization's behalf. Reporting to CISA only satisfies legally required reporting requirements to the extent that the reporting requirement explicitly provides that
976	reporting to or through CISA is a means of compliance.)
977	A. [CUI]{Conditional} [FISMA Req] (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 <sup>rd</sup> party) (DESIGN NOTE: Repeat the
983 984	following for each notification entity selected, can also be more than one entry per category, e.g., law enforcement can be local and federal notifications)
985	a. Entity Name (Design Note: Provide check box to allow the reporter to identify if
986	this value is the same as the impacted entity's name. If box is checked, copy the
987	impacted entity's name to this variable)
988	1. [CUI]Point of contact name
989	i. First
990	ii. Last
991 992	<ul><li>2. Email address(es) of Point of Contact</li><li>3. Phone number(s)</li></ul>
993	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
994	offset>)
995	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM
996	<ul><li><utc offset="">)</utc></li></ul>
997	d. Case/incident/report number provided (if applicable)
998	2. Inspector general (DESIGN NOTE: Repeat the following sub entries "a through d" for each
999	notification entity selected, other than the information owner. There can also be more than one
1000	entry "a through d" per category, e.g., law enforcement can be local and federal.)
1001	a. Entity Name
1002	1. [CUI]Point of contact name

<sup>26</sup> 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 non-authorized personnel (e.g., information with customer credit card or social security numbers thrown in local dumpster or lost mail containing PII).

1003	i. First
1004	ii. Last
1005	2. Email address(es) of Point of Contact
1006	3. Phone number(s)
1007	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1008	offset>)
1009	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1010	<utc offset="">)</utc>
1011	d. Case/incident/report number provided (if applicable)
1012	3. Legal counsel
1013	4. Law enforcement
1014	5. Regulatory agency
1015	6. Privacy officials
1016	7. Security staff
1017	8. System owners
1018	9. Other (DESIGN NOTE: Repeat the following sub entries a through d for each notification
1019	entity selected, other than the information owner. There can also be more than one entry "a
1020	through d" per category, e.g., law enforcement can be local and federal.)
1021	a. Entity Name
1022	1. [CUI]Point of contact name
1023	i. First
1024	ii. Last
1025	2. Email address(es) of Point of Contact
1026	3. Phone number(s)
1027	4. Position/Title
1028	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1029	offset>)
1030	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1031	<utc offset="">)</utc>
1032	d. Case/incident/report number provided (if applicable)
1033	
1034	B. [CUI] {Conditional} [FISMA Req] (DESIGN NOTE: If Yes) Have you already, or are
1035	you planning to report this incident to any federal government agency other than
1036	CISA?
1037	1. [If Yes] Which agency? (DESIGN NOTE: Select from agency list in Appendix 5)
1038	a. Entity Name (Design Note: Provide check box to allow the reporter to identify if
1039	this value is the same as the impacted entity's name. If box is checked, copy the
1040	impacted entity's name to this variable)
1041	1. [CUI]Point of contact name
1042	i. First
1043	ii. Last
1044	2. Email address(es) of Point of Contact
1045	3. Phone number(s)
1046	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1047	offset>)
1048	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1049	<utc offset="">)</utc>

1050	d. Case/incident/report number provided (if applicable)
1051	C. (DESIGN NOTE: All other reporters not FISMA) [CUI] {Conditional} [Op] (DESIGN NOTE:
1052	If Yes) Please list the entities you will, or did, report to. (DISPLAY NOTE: This
1053	information may be helpful for CISA to understand if there are other entities that CISA may need to
1054	collaborate with or allow for special considerations during any incident response efforts.)
1055	1. Information owners (examples include information managed by
1056	affected/reporting entity (e.g., cloud provider) but owned by
1057	affected/reporting entity's customer/client) (DESIGN NOTE: Repeat the following for
1058	each notification entity selected, can also be more than one entry per category, e.g., law
1059	enforcement can be local and federal notifications.)
1060 1061	a. Entity Name (Design Note: Provide check box to allow the reporter to identify if this value is the same as the impacted entity's name. If box is checked, copy the
1062	impacted entity's name to this variable)
1063	1. [CUI]Point of contact name
1064	i. First
1065	ii. Last
1066	2. Email address(es) of Point of Contact
1067	3. Phone number(s)
1068	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1069	offset>)
1009	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1070 1071	<ul><li><utc offset="">)</utc></li></ul>
1071 1072	d. Case/incident/report number provided (if applicable)
1073 1074	2. Law enforcement (DESIGN NOTE: Repeat the following sub entries a through d for each notification entity selected, other than the information owner. There can also be more than one
1075	entry "a through d" per category, e.g., law enforcement can be local and federal.)
1076	a. Entity Name
1077	1. [CUI]Point of contact name
1078	i. First
1079	ii. Last
1080	2. Email address(es) of Point of Contact
1081	3. Phone number(s)
1082	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1083	offset>)
1084	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -
1085	<utc offset="">)</utc>
1086	d. Case/incident/report number provided (if applicable)
1087	3. Regulatory agency
1088	4. Other federal agencies
1089	a. If selected, which agency? (DESIGN NOTE: Select from agency list in
1090	Appendix 5)
1091	5. Other (DESIGN NOTE: Repeat the following sub entries a through d for each notification
1092	entity selected, other than the information owner. There can also be more than one entry "a
1093	through d" per category, e.g., law enforcement can be local and federal.)
1094	a. Entity Name
1095	1. [CUI]Point of contact name
1096	i. First
1097	ii. Last
1098	2. Email address(es) of Point of Contact

1099	3. Phone number(s)
1100	4. Position/Title
1101	b. Already notified: Date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
1102	offset>)
1103	c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM
1104	<utc offset="">)</utc>
1105	d. Case/incident/report number provided (if applicable)
1106	j. Incident: Severity Assessments
1107	Confidentiality, Integrity, Availability (CIA) Assessment <sup>27</sup>
1108	26. [RA] (DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event-
1109	Incident FLAG for FISMA reporters only. If Q26 A-C are answered "no", that terminates the rest of the
1110	Incident Questions for a FISMA reporter, and the FISMA reporter is directed towards filling out "Event
1111	Reporting" only.) At this time, is this incident known to either imminently <sup>28</sup> or actually
1112	jeopardize, without lawful authority, any of the following relating to either
1113	information or an information system? (select all that apply) (DESIGN NOTE: For non-
1114	FISMA reports, if "unsure/None" selected for all three CIA questions, then DISPLAY NOTE: You have no
1115	indicated an impact on at least one of the three areas of confidentiality, integrity, or availability per the
1116	definition of an incident.)
1117	A. Confidentiality. <sup>29</sup> [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Have
1118	radio button for all)
1119	B. Integrity, <sup>30</sup> [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Have radio
1120	button for all)
1121	C. Availability. <sup>31</sup> [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Have
1122	radio button for all)
1123	

<sup>27</sup> 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

<sup>&</sup>lt;sup>28</sup> 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}]

<sup>&</sup>lt;sup>29</sup> "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.]

<sup>&</sup>lt;sup>30</sup> "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.]

<sup>&</sup>lt;sup>31</sup> "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)]

1124	Violation of Law and Policy
1125	27. [RA] At this time, does this incident constitute an imminent or actual violation of law,
1126	security policies, security procedures, or acceptable use policies? (Yes/No) (DESIGN
1127	NOTE: If Yes) Please make selection(s) below
1128	A. Violation of law [] imminently; [] actually; [] unsure; [] none (DESIGN NOTE: Single
1129	select have radio button for all.)
1130	B. Security policies and/or procedures [] imminently; [] actually; [] unsure; [] none
1131	(DESIGN NOTE: Single select have radio button for all.)
1132	C. Acceptable use policies [] imminently; [] actually; [] unsure; [] none (DESIGN
1133	NOTE: Single select have radio button for all.)
1134	
1135	Incident: High-Level Impacts
1136	Public Impacts
1137	National US Impacts
1138 1139	(DESIGN NOTE: Major Incident Flag Questions. Any "Yes" answer here is used to determine if the reporter is reporting a major incident as defined by FISMA in the next question by adding in "Demonstrable Harm" for
1140	those that selected "Yes" here.)
1141	28. [Op] + [FISMA Req] To the best of your knowledge, does the incident likely impact
1142	any of the following? (Select all that apply)
1143	A. National security interests of the United States
1144	B. Foreign relations of the United States
1145	C. Economy of the United States
1146	D. Public confidence of the American people
1147	E. Civil liberties of the American people
1148	F. Public health and safety of the American people
1149 1150 1151 1152 1153	(DESIGN NOTE: Major Incident - FLAG Questions: For "Q29" question, users should see all options from "Q 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 harm" severity, will indicate that the incident is considered a major incident" under FISMA reporting.)  [Op] + [FISMA Req] At the time of this report, of the likely impacts of this incident
1154	selected above, are any of them likely to result in <b>demonstrable harm</b> to the United
1155	States? (DISPLAY NOTE: Select those that are likely to result in demonstrable harm.) (DESIGN NOTE:
1156	Skip this question if nothing selected in question 28. Display list containing only the options the user
1157	selected in Q28. Provide user a "check box" in Q29 so they can indicate which options represent
1158	"demonstrable harm.")
1159	Regional Impacts (Local to Global)  29. [Op] + [RR] To the best of your knowledge, describe the extent of the incident's
1160	impact on the population/geographic region
1161	
1162	A. Internal/site-specific (Impacts are felt by the impacted entity or a particular
1163	facility or site, but not externally)  D. Local (Impact is limited to antition on systematic in the immediate area (e.g., towns
1164	B. Local (Impact is limited to entities or customers in the immediate area (e.g., town,
1165	city) external to the core business of the affected entity)
1166	C. State/territory-wide

1167	D. Regional
1168	E. Multi-regional
1169	F. National
1170	G. Multi-national
1171	H. Global
1172	I. Unknown
1173	
1174	Breach <sup>32</sup> Severity Impacts
1175	30. [Op] + [FISMA Req] At this time, has the incident resulted in any confirmed
1176	unauthorized access to personally identifiable information? (Yes/No) (DESIGN NOTE: If
1177	Yes, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions
1178	"access due" and "accessed by" only if "Yes",)
1179	A. Was the access due to (select all that apply):
1180	1. Loss of control
1181	2. Compromise
1182	3. Unauthorized disclosure
1183	4. Unauthorized acquisition
1184	B. Was the information accessed by (select all that apply):
1185	1. A person other than an authorized user
1186	2. An authorized user who accessed the personally identifiable information for
1187	an other-than-authorized purpose
1188	31. {Conditional}[Op] + [FISMA Req] (DESIGN NOTE: Do not ask this question if the "Confirmed
1189	Unauthorized Access" question yields a positive selection response. Only ask if previous response to
1190	"confirmed" = "No") At this time, has the incident resulted in any potential unauthorized
1191	access to personally identifiable information? (Yes/No) (DESIGN NOTE: If Yes, flag as
1192	Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access
1193	due" and "accessed by" only if "Yes".)
1194	A. Was the potential unauthorized access due to: (select all that apply)
1195	1. Loss of control
1196	2. Compromise
1197	3. Unauthorized disclosure
1198	4. Unauthorized acquisition
1199	B. Was the information potentially accessed by (select all that apply)
1200	1. A person other than an authorized user
1201	2. An authorized user who accessed the personally identifiable information for
1202	an other-than-authorized purpose
1203 1204	(DESIGN NOTE: Following responses for Q31 and Q32, if breach severity "confirmed or potential unauthorized access" = Yes, DISPLAY on "POP UP SCREEN", display note to reporter: "You have indicated you have had an

<sup>&</sup>lt;sup>32</sup> 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

1205 1206	actual or potential breach and impacts to PII. You will be given an opportunity to provide more details on the types of PII impacted later in this report.")
1207	Major Incident Severity Determination (FISMA Only)
1208	32. [FISMA Req] At the time of this report, did any of the following occur involving
1209	personally identifiable information? (DESIGN NOTE: Major Incident - FLAG Question: Only
1210	appears if Breach Severity "Confirmed or Potential Unauthorized Access" = Yes. If any "100,000" field is
1211	answered yes below, flag as major incident. (DESIGN NOTE: a FISMA major Incident = a significant
1212	cyber incident) (DESIGN NOTE: multi select) (DISPLAY NOTE: Select all that apply)
1213	A. [] Unauthorized modification
1214	1. (DESIGN NOTE: If selected display following:)
1215	a. Was this a [] potential or [] actual occurrence?
1216	b. Did this occurrence or potential occurrence involve the PII of
1217	100,000 or more people? (Y/N)
1218	B. [] Unauthorized deletion
1219	1. (DESIGN NOTE: If selected display following:)
1220	a. Was this a [] potential or [] actual occurrence?
1221	b. Did this occurrence or potential occurrence involve the PII of
1222	100,000 or more people? (Y/N)
1223	C. [] Unauthorized exfiltration
1224	1. (DESIGN NOTE: If selected display following:)
1225	a. Was this a [] potential or [] actual occurrence?
1226	b. Did this occurrence or potential occurrence involve the PII of
1227	100,000 or more people? (Y/N)
1228	D. [] Unauthorized access
1229	1. (DESIGN NOTE: If selected display following:)
1230	a. Was this a [] potential or [] actual occurrence?
1231	b. Did this occurrence or potential occurrence involve the PII of
1232	100,000 or more people? (Y/N)
1233	33. [FISMA Req] At the time of this report, has your answer to any item within the
1234	preceding "major incident severity" questions changed since a previous report?
1235	(Yes/No) (DESIGN NOTE: Only show if "supplemental/update" or "post-incident" report is selected)
1236	A. (DESIGN NOTE: If Yes) Did this change cause the report to (Select one response)
1237	1. [] Upgrade to a major incident?
1238	a. Please provide additional context for the change
1239	2. [] Downgrade from a major incident?
1240	a. Please provide additional context for the change
1241	3. [] No change in major incident determination (the incident was either
1242	previously not determined to be a major incident and remains as such, or was
1243	previously determined to be a major incident and remains as such)
1244	a. Please provide additional context

1245	34. [FISMA Req] (DESIGN NOTE: Only asked of FISMA reporters if the incident has been indicated as a
1246	"Major Incident" per thresholds in questions 29 and/or 33.) Has this incident been reported to
1247	Congress? (Yes/No)
1248	Public Health and Safety Impacts
1249	35. [Op] + [RR] To the best of your knowledge, what is the current impact of this
1250	incident on public health? (DISPLAY NOTE: Public health impacts are defined as "impacts on an
1251	affected population measured based on new and increased death, disease, injury, and disability." Impacts to
1252	access to medical care are considered public safety impacts, which are addressed in a later question.)
1253	A. No impact – Incident has no impact on public health
1254	B. Low impact – Incident has resulted in one or more minor injuries and/or
1255	temporary disabilities that have not required emergency response (e.g., minor
1256	symptoms prompting self-care)
1257	C. Moderate impact – Incident has resulted in one or more moderate injuries and/or
1258	lasting disabilities that have required emergency response and/or risk (e.g., easily
1259	treated symptoms or hospital diagnostic visits)
1260	D. High impact – Incident has resulted in one or more serious injuries that have
1261	required emergency response and/or permanent disabilities
1262	E. Critical impact – Incident has resulted in one or more deaths
1263	F. Unknown impact – Reporter does not have information required to assess the
1264	impact of the incident on public health
1265	36. [Op] + [RR] To the best of your knowledge, what is the current impact of this
1266	incident on public safety? (DISPLAY NOTE: Public safety impacts are defined as "Impact measured
1267	based on an affected population's ability to obtain shelter (e.g., temporary housing, temperature
1268 1269	regulation), healthcare (e.g., emergency response services, open hospital beds), and lifeline resources (e.g., clean air and water, nutrition, hydration, communication – phone and internet service) and to maintain
1270	physical safety (e.g., data breaches that threaten individual safety).")
1271	A. No impact – Incident has no impact on public safety
1272	B. Low impact – Incident has minimal impact on public safety (e.g., limited, short
1273	term disruption of essential services and/or lifeline resources – phone and internet
1274	service, electricity, water)
1275	C. Moderate impact – Incident has more extensive impact on public safety (e.g.,
1276	longer-term disruption of lifeline resources such as phone, internet, electricity,
1277	and water; healthcare and shelter impacts/disruptions from loss of electricity for
1278	extended period)
1279	D. High impact – Incident has severe impact on public safety (e.g., evacuation and
1280	temporary housing of displaced communities; immediate threats to physical safety
1281	of the public; extended disruption of essential services; stress on healthcare
1282	resources; water and air contamination)
1283	E. Critical impact – Incident has catastrophic impact on public safety (e.g., long-term
1284	environmental contamination; cessation of essential services such as law
1285	enforcement and healthcare; societal instability)
	•

1286	F. Unknown impact – Reporter does not have the information required to assess the
1287	impact of the incident on public safety
1288	Indirect Impacts
1289	37. [Op] + [RR] To the best of your knowledge, were/are there any indirect (or
1290	secondary) impacts to other critical infrastructure sector(s). <sup>33</sup> ? (Yes/No)
1291	A. (DESIGN NOTE: If Yes) Please select the appropriate critical infrastructure sector and
1292	the appropriate critical infrastructure subsector(s) (if applicable) that were
1293	indirectly impacted, and indicate what type of impact (functional, informational,
1294	economic and/or physical). (DESIGN NOTE: See Appendix 4 for complete critical
1295	infrastructure sector and subsector list.)
1296	(DESIGN NOTE: Multi select) (DISPLAY NOTE: Indirect impact is defined as "an effect that is not a
1297	direct consequence of an incident, but is caused by a direct consequence, subsequent cascading effects,
1298	and/or related decisions. For example, if an electric power plant is the victim of a malicious cyber incident,
1299	directly impacting the provision of energy sector services (in this case, electricity), other local or regional
1300 1301	sectors that are dependent on that electricity – e.g., commercial facilities and critical manufacturing – may experience indirect impacts.")
1302	1. Chemical (DESIGN NOTE: Multi select include any subsector lists from Appendix 4 as
1303 1304	necessary and repeat the four "impact" selections per critical infrastructure-cross sector and/or subsector instance selected)
1305 1306	a. Type(s) of Impact: (DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all
1300 1307	that apply) 1. Functional impact <sup>34</sup>
1308	2. Informational impact <sup>35</sup>
1309	3. Economic impact. <sup>36</sup>
1310	4. Physical impact <sup>37</sup>
1311	b. Subsector list (if available) here: (DESIGN NOTE: Multi select) (DISPLAY
1312	NOTE: Select all that apply)
1313	1. Type(s) of Impact:
1314	i. Functional impact
1315	ii. Informational impact
1316	iii. Economic impact
	- -
_	

<sup>&</sup>lt;sup>33</sup> https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

<sup>&</sup>lt;sup>34</sup> 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). CISA National Cyber Incident Scoring System (NCISS) | CISA

<sup>35</sup> 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). CISA National Cyber Incident Scoring System (NCISS) | CISA

<sup>&</sup>lt;sup>36</sup> 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, https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE Cost of Cyber Incidents Study-FINAL 508.pdf

<sup>&</sup>lt;sup>37</sup> 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.

1317	iv. Physical impact
1318	2. Commercial Facilities
1319	3. Communications
1320	4. Critical Manufacturing
1321	5. Dams
1322	6. Defense Industrial Base
1323	7. Emergency Services
1324	8. Energy
1325	9. Financial Services
1326	10. Food and Agriculture
1327	11. Government Facilities
1328	12. Healthcare and Public Health
1329	13. Information Technology
1330	14. Nuclear Reactors, Materials, and Waste
1331	15. Transportation Systems
1332	16. Water and Wastewater Systems
1333	17. Unknown
1334	20 FO 1 - FDD1T 4 1 4 6 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1335	38. [Op] + [RR] To the best of your knowledge, what is the current functional,
1336	informational, economic, and/or physical impact to other third parties that are not
1337	entities in a critical infrastructure sector? (DESIGN NOTE: Multi select)
1338	A. Functional impact
1339	1. Not applicable, there is no possibility of indirect functional impact to entities
1340	not in a critical infrastructure sector
1341	2. No impact at this time
1342	3. Low impact
1343	4. Moderate impact
1344	5. High impact
1345	6. Critical
1346	7. Unknown
1347	B. Informational impact
1348	1. Not applicable, there is no possibility of indirect informational impact to
1349	entities not in a critical infrastructure sector
1350	2. No impact at this time
1351	3. Low impact
1352	4. Moderate impact
1353	5. High impact
1354	6. Critical
1355	7. Unknown
1356	C. Economic impact

4057	1	No. 1: 11 4 1 1 11 12 12 12 12 12 12 12 12 12 12 12
1357	1.	Not applicable, there is no possibility of indirect economic impact to entities
1358	_	not in a critical infrastructure sector
1359	2.	No impact at this time
1360	3.	Low impact
1361	4.	Moderate impact
1362	5.	High impact
1363	6.	Critical
1364	7.	Unknown
1365	D. Phy	ysical impact
1366	-	Not applicable, there is no possibility of indirect physical impact to entities
1367		not in a critical infrastructure sector
1368	2.	No impact at this time
1369	3.	Low impact
1370	4.	Moderate impact
1371	5.	High impact
1372	6.	Critical
1373	7.	Unknown
1374	Impacts	Internal to the Entity
1375	Func	tional Impacts to Entity
1376		[RR] To the best of your knowledge, what is the current functional impact <sup>38</sup>
1377		incident?
1378	A. No	impact to both non-critical and critical services (DISPLAY NOTE: Incident has no
1379		act.)
1380	B. No	n-critical services:
1381	1.	No impact to non-critical services (DISPLAY NOTE: Incident has no impact to non-
1382		critical services.)
1383	2.	· · · · · · · · · · · · · · · · · · ·
1384		business or on delivery to entity customers.)
1385	3.	Moderate impact to non-critical services (DISPLAY NOTE: Moderate impact to non-
1386		critical services. Some small level of impact to non-critical systems and services.)
1387	4.	
1388	~	critical services. A non-critical service or system has a significant impact.)
1389	5.	Critical impact to non-critical services (DISPLAY NOTE: Denial of non-critical
1390		services. A non-critical system's access is denied, or system's functionality is destroyed.)
1391		Unknown
1392		tical services:
1393	1.	No impact to critical services (DISPLAY NOTE: Incident has no impact to critical
1394		services )

<sup>38</sup> **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>

1395	2. Low impact to critical services (DISPLAY NOTE: Incident has low impact on any
1396	industrial control systems (ICS) or on delivery of critical services to entity customers.)
1397	3. Moderate impact to critical services. <sup>39</sup> (DISPLAY NOTE: Moderate impact to a critical
1398	system or service (e.g., email, active directory).)
1399	4. High impact to critical services (DISPLAY NOTE: A critical system has a significant
1400	impact (e.g., local administrative account compromise).)
1401	5. Critical impact to critical services (DISPLAY NOTE: Denial of critical services/loss of
1402	control. A critical system has been rendered unavailable.)
1403	6. Unknown
1404	40. $\{Conditional\} [Op] + [RR] (DESIGN NOTE: Only display question if response to "Functional")$
1405	Impact" yields a "Low, Moderate, High, Critical, or Unknown" selection by the reporter for either non-
1406	critical or critical services). Please select (one) the most severe location any observed
1407	disruption in your entity's non-critical business or critical system networks from
1408	within your environment from this list:
1409	A. Business demilitarized zone (DMZ) (Activity was observed in the business
1410	network's demilitarized zone (DMZ))
1411	B. Business network (Activity was observed in the business or corporate network of
1412	the entity; these systems would include corporate user workstations, application
1413	servers, and other non-core management systems)
1414	C. Business network management (Activity was observed in business network
1415	management systems such as administrative user workstations, active directory
1416	servers, or other trust stores)
1417	D. Critical system DMZ (Activity was observed in the DMZ that exists between the
1418	business network and a critical system network. These systems may be internally
1419	facing services such as SharePoint sites, financial systems, or relay "jump" boxes
1420	into more critical systems.)
1421	E. Critical system management (Activity was observed in high-level critical systems
1422	management such as human-machine interfaces in Industrial Control Systems)
1423	F. Critical systems (Activity was observed in the critical systems that operate critical
1424	
	processes.)
1425	G. Unknown
1426	H. Other [describe] (DESIGN NOTE: Open Text)
1427	Informational Impacts to Entity
1428	41. [Op] + [RR] To the best of your knowledge, what is the current informational
1429	impact. <sup>40</sup> of this incident?

<sup>&</sup>lt;sup>39</sup> **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 https://www.dhs.gov/publication/dhs-lexicon* 

<sup>&</sup>lt;sup>40</sup> **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

1430	A. No impact
1431	B. Low impact
1432	C. Moderate impact
1433	D. High impact
1434	E. Critical impact (unrecoverable)
1435	F. Unknown
1436	Physical Impacts to Entity
1437	42. [Op] + [RR] To the best of your knowledge, what is the current physical impact <sup>41</sup> of
1438	this incident?
1439	A. No physical impact to both property and systems
1440	B. Physical impacts to property:
1441	1. No impact to non-critical and critical property
1442	2. Low impact to property (DISPLAY NOTE: Damage to non-critical property)
1443	3. Moderate impact to property (DISPLAY NOTE: Damage to critical property. 42)
1444	4. High impact to property (DISPLAY NOTE: Destruction of non-critical property)
1445	5. Critical impact to property (DISPLAY NOTE: Destruction of critical property)
1446	6. Unknown
1447	C. Physical impacts to systems:
1448	1. No impact to non-critical and critical systems
1449	2. Low impact to systems (DISPLAY NOTE: Damage to non-critical systems)
1450	3. Moderate impact to systems (DISPLAY NOTE: Damage to critical systems)
1451	4. High impact to systems (DISPLAY NOTE: Destruction of non-critical systems)
1452	5. Critical impact to systems (DISPLAY NOTE: Destruction of critical systems)
1453	6. Unknown
1454	Economic Impacts to Entity
1455	43. [Op] + [RR] To the best of your knowledge, what is the current economic impact <sup>43</sup> of
1456	this incident? (DISPLAY NOTE: Estimate any costs or losses associated with the categories of economic

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>

<sup>&</sup>lt;sup>41</sup> **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.

<sup>&</sup>lt;sup>42</sup> **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 https://www.dhs.gov/publication/dhs-lexicon* 

<sup>&</sup>lt;sup>43</sup> **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, <a href="https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE">https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE</a> Cost of Cyber Incidents Study-FINAL 508.pdf

1457 1458	impacts listed below. If you require further clarity on the meaning of these categories of economic impacts, see the CISA report: "Cost of Cyber Incident.". <sup>44</sup> )
1459	A. Incident investigation and forensic analysis
1460	1. Please provide estimates in U.S. dollars for each applicable category of
1461	economic impact (use a range from minimum to maximum where uncertain,
1462	or the same for both if known) (DESIGN NOTE: Repeated for each selected)
1463	B. Incident response and containment (including direct response, cleanup, and
1464	recovery costs)
1465	C. Lost revenue or productivity
1466	D. Theft, fraud, and direct financial losses (including any ransomware payments
1467	disbursed)
1468	E. Legal fees and regulatory fines
1469	F. Victim notification and protection services
1470	G. Other Losses (e.g., Loss of Intellectual Property)
1471	k. Incident Details
4.470	Incident: Details by Stage
1472 1473	
1473	(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
1475	Security Incident Handling Guide). 45 Please note, you can be in multiple stages of an incident response at one time
1476	and can revisit any incident stage-specific section of this report at any point if there is new information to report.)
1477	l. Identification and Detection (I/D) Stage
1478	
1479	Incident Stage (I/D): Ransomware and Cyber Extortion
1480	(DESIGN NOTE: Executes if incident is flagged as a Ransomware Incident in "Incident Type
1481	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: Multi select, then drop down for more refined selections within each main
	category, dropdown lists are in Appendix 3.) (DESIGN NOTE: Must have the drop lists "searchable" by key words by type and subtype categories.) (DISPLAY NOTE: Select all that apply)
	<ul> <li>→ A. Malware [e.g., ransomware, DDOS, etc.]</li> <li>B. Human (or Technology) Errors [e.g., loss of equipment, system</li> </ul>
1482	misconfiguration, mishandling of sensitive and/or PII documentation, etc.]
1483	Initial Ransom Demand Details
1484	44. [RC] Please provide the following details about the ransom demand associated with
1485	this incident:
1486	A. [C-15] [Op] + [FISMA Req] Text of ransom demand(s) (DESIGN NOTE: Open text)
1487	B. [C-15] [Op] + [FISMA Req] Screenshot of ransom note(s) or copy of the email(s)
1488	C. [C-15] [Op] + [FISMA Req] Ransomware variant used (if known)

 $<sup>^{44}</sup>$  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

1489	D. [C-15] [Op] + [FISMA Req] Amount of ransom demand
1490	E. [C-15] [Op] + [FISMA Req] Currency type of ransom demand, including virtual
1491	currency
1492	F. [C-15] [Op] + [FISMA Req] Text of ransom payment instructions (if not already
1493	included in response to A, above) (DESIGN NOTE: Allow for a response to be "Same as
1494	response A", this is an open text otherwise.)
1495	G. [C-15] [Op] + [FISMA Req] Deadline given to pay ransom. Please provide the
1496	Date and Time (yyyy-mm-dd HH:MM - <utc offset="">) (DISPLAY NOTE: This could be</utc>
1497	a time in the future at time of report.)
1498	H. [C-15] [Op] + [FISMA Req] Description of any additional communications
1499	between the threat actors and either the impacted entity or a third party authorized
1500	to act on its behalf (e.g., phone conversations)
1501	I. [Op] + [FISMA Req] Does your organization have insurance that covers
1502	ransomware demand payments? (Yes/No)
1503	1. (DESIGN NOTE: If Yes) Please provide insurance company details
1504	a. Name
1505	b. Email address
1506	1. Unknown
1507	c. Website
1508	1. Unknown
1509	d. Physical address
1510	1. Street name and number
1511	2. Postal code
1512	3. City
1513	4. State
1514	5. Country
1515	e. Other contact information
1516	f. Insurance annual premium amount (DISPLAY NOTE: Primary carrier
1517	amounts if applicable, and if there is a separate cost for "ransom payments" only
1518	include that amount, otherwise total cost is acceptable.)
1519	1. Amount
1520	i. [] Select if primary carrier amount
1521	ii. [] Ransom coverage only [] Total coverage (DESIGN
1522	NOTE: Select one)
1523	2. Does the impacted entity plan on seeking, or has it already sought coverage
1524	from its insurers for this incident? (Yes/No)
1525	Ransom Payment Details
1526	J. Ransom Payment Details
1527	1. [Op] + [FISMA Req] Was a ransom paid? (Yes/No)
1528	a. $\{Conditional\} + [OP] + [RR] (DESIGN NOTE: If Yes) Did your ransom$
1520	nayment incurence cover the incident? (Vec/No) (DESIGN NOTE)

1530	Only ask if answered "Yes" to having ransomware insurance and planning to seek
1531	coverage.)
1532	2. {Conditional} [Op] + [FISMA Req] If ransom was paid, provide the
1533	following (DESIGN NOTE: Set Payment Count as 1.)
1534	(DESIGN NOTE: ====================================
1535	a. [CUI] [Op] + [FISMA Req] <b>Negotiation Details:</b> Did you use a
1536	negotiation agent? (Yes/No), {Conditional} + [Op] + [FISMA
1537	Req] (DESIGN NOTE: If Yes) Provide
1538	1. [CUI]Negotiation agent point of contact
1539	i. [CUI]If person
1540	1. First
1541	2. Last
1542	3. Phone number(s)
1543	4. Email address(es)
1544	5. Position/title
1545	ii. If entity
1546	1. Name
1547	2. Email address
1548	i. Unknown
1549	3. Website
1550	i. Unknown
1551	4. Physical address
1552	i. Street name and number
1553	ii. Postal code
1554	iii. City
1555	iv. State
1556	v. Country
1557	5. Other contact information
1558	(DISPLAY NOTE: When a ransom payment is made, the victim sharing information regarding the payer (the
1559	person paying the ransom payment), the recipient (the person receiving the ransom payment), and how the
1560	transaction occurred can enable a more effective federal response to a ransom (or extortion) incident. CISA
1561 1562	recognizes there may be multiple transactions over the course of the incident; this form will solicit the (potentially) unique details for each transaction separately.)
1563	b. [CUI] [Op] + [FISMA Req] Is the payer an individual or entity?
1564	(Select: Individual/entity) (DESIGN NOTE: Single select)
1565	1. [CUI]{Conditional} + [Op] + [FISMA Req] [Payer] (DESIGN
1566	NOTE: If Individual):
1567	i. First
1568	ii. Last
1569	iii. Phone number(s)
1570	iv. Email address(es)
1571	v. Position/title
1572	vi. Organization
13/2	vi. Organization
	$P_{\text{aga}}/2$ of 120

2. [CUI]{Conditional} + [Op] + [FISMA Req] [Payer] (DESIGN
NOTE: If Entity):
i. Entity name
ii. [CUI] Point of contact
1. First
2. Last
3. Phone number(s)
4. Email address(es)
5. Position/title
iii. Entity email address
1. Unknown
iv. Website
1. Unknown
v. Physical address
1. Street name and number
2. Postal code
3. City
4. State
5. Country
vi. [CUI] Other contact information
3. [CUI] [Op] + [FISMA Req] [Payer] Details of transaction per
payment made to date: (DISPLAY NOTE: This is from the Payer's
perspective. Additionally, the total ransom/extortion amount could be spread
among multiple payments and different methods.)
i. Date and time payment was disbursed from the payer
making the ransom payment to satisfy the ransom
demand
ii. Currency type (traditional, virtual/digital asset, or other)
1. Currency
2. Other, provide description (DESIGN NOTE: Open text)
iii. Amount of payment (may be equal to or different from
the actual demand)
1. In virtual/digital asset
2. In US dollar value at the time of the transaction
iv. [CUI] For transactions that involved a bank or another
type of financial institution (e.g., in facilitating the
payment)
1. Name of bank or financial institution
2. Address of bank or financial institution
i. Street name and number
ii. Postal code

1614	iii. City
1615	iv. State
1616	v. Country
1617	3. Name(s) on the account
1618	4. Account number
1619	5. Routing number
1620	i. Origin
1621	v. [CUI] If virtual (e.g., crypto) currencies were used:
1622	1. Service used to
1623	i. Purchase the currency
1624	ii. Store the currency
1625	iii. Transmit the currency
1626	2. [CUI] Transaction ID (e.g., transaction hash), if
1627	known
1628	3. [CUI] Virtual (crypto) currency address(es)
1629	i. Payer addresses
1630	vi. Other method of paying the ransom / extortion demands
1631	1. [CUI] Describe the method
1632	vii. If the transaction occurred at a physical location, please
1633	provide
1634	1. Address of transaction
1635	i. Geographical point of interest (location)
1636	ii. Street name and number
1637	iii. Postal code
1638	iv. City
1639	v. State
1640	vi. Country
1641	2. Any other physical location characteristics describe
1642	here:
1643	c. [CUI] [Op] + [FISMA Req] To the best of your knowledge, is the
1644	recipient an individual, entity, or group?
1645	Select: []Individual []Entity []Group []Unknown (DESIGN NOTE:
1646	Skip "point of contact" info if "Unknown" selected) (DESIGN NOTE: Single
1647	select)
1648	1. [CUI] [Op] [FISMA Req if selected] [Recipient] (DESIGN
1649	NOTE: If Individual) Please provide the following information to
1650	the extent known:
1651	i. First
1652	ii. Middle
1653	iii. Last
1654	iv. Suffix

1655	v. Phone number(s)
1656	vi. Email address(es)
1657	vii. Social media information
1658	viii. Position/title
1659	2. [CUI] [Op] + [FISMA Req if selected] [Recipient] (DESIGN
1660	NOTE: If Entity/Group) Please provide the following information
1661	to the extent known:
1662	i. Name
1663	ii. [CUI] Point of contact at entity
1664	1. First
1665	2. Middle
1666	3. Last
1667	4. Suffix
1668	5. Phone number(s)
1669	6. Email address(es)
1670	7. Position/title
1671	iii. Entity email address
1672	iv. Entity social media information
1673	v. Entity website
1674	vi. Physical address
1675	1. Street name
1676	2. Street number
1677	3. Postal code
1678	4. City
1679	5. State
1680	6. Country
1681	vii. Any other contact information describe here:
1682	d. [CUI] [Op] + [FISMA Req if available] [Recipient] Details of
1683	transaction per payment: (DISPLAY NOTE: This is from the Recipient's
1684	perspective. Additionally, the total ransom/extortion amount could be spread among
1685	multiple payments and different methods.)
1686	1. Date and time of ransom payment
1687	2. Currency type (traditional, virtual/digital, or other)
1688	i. Currency
1689	ii. Other, provide description (DESIGN NOTE: Open text)
1690	3. Amount of ransom payment (may be equal to or different
1691	from the actual demand)
1692	i. In virtual/digital asset
1693	ii. In US dollars
1694	4. [CUI] For transaction(s) that involved a bank or another type
1695	of financial institution:

1696	i. Name of bank or financial institution
1697	ii. Address of bank or financial institution
1698	1. Street name and number
1699	2. Postal code
1700	3. City
	•
1701	4. State
1702	5. Country
1703	iii. Name(s) on the account
1704	iv. Account number
1705	v. Routing number
1706	1. Destination
1707	5. If virtual (e.g., crypto) currencies were used
1708	i. Service used to
1709	1. Purchase the currency
1710	2. Store the currency
1711	3. Transmit the currency
1712	ii. [CUI] Transaction ID (e.g., transaction hash), if known
1713	iii. [CUI] Virtual (crypto) currency address(es)
1714	1. Payee addresses
1715	K. [Op] + [FISMA Req] Identifying payment installments
1716	1. Were multiple payments made (e.g., installments, differing methods [some
1717	physical cash, some virtual])? (Yes/No) (Design Note: If Yes, complete another session
1718	of "payment details", associate payment # to installment # + 1. Provide an option to copy over
1719	from the first payment the information since it may be all the same except for date/time.)
1720	(DESIGN NOTE:^^^^^=End of Ransom Payment Details=^^^^^^)
1721	Results of Ransom Incident
1722	L. [CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident
1723	1. Were you provided with decryption capabilities (e.g., keys) by the threat
1724	actor? (Yes/No)
1725	a. (DESIGN NOTE: If Yes) Did the keys work?
1726	b. What percentage of the files were recoverable (approximate)?
1727	2. To the best of your knowledge, was any data stolen? (Yes/No/Unsure)
1728	(DESIGN NOTE: If Yes or Unsure):
1729	a. [CUI] Describe the type of data stolen or suspected to have been
1730	stolen, to the best of your knowledge (DESIGN NOTE: Open text)
1731	b. [CUI] Did the threat actors leak any stolen data, to the best of your
1732	knowledge? (Yes/No) (DESIGN NOTE: If Yes) [describe]
1733	c. [CUI] Did the threat actors use any other pressure tactics, such as
1734	contacting third parties to inform them of the compromise?
1735	(Yes/No) (DESIGN NOTE: If Yes) [describe].
1736	3. [CUI] Describe any additional results of the ransom incident.
	c. [] =) against resume of the temporal metaeum

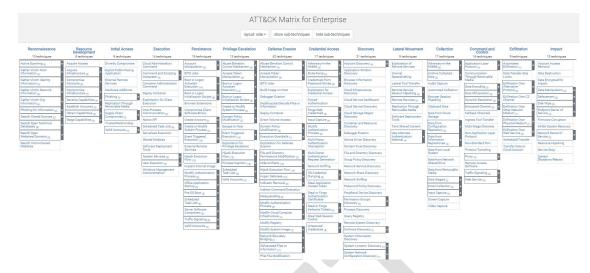
1/3/	M. $[Op] + [FISMA Req]$ Did you experience follow-on attempts by threat actors to
1738	extort money or services? (Yes/No)
1739	{Conditional} [Op] + [FISMA Req] (DESIGN NOTE: If Yes) Did you pay the
1740	additional ransom or extortion demands? (Yes/No)
1741	(DESIGN NOTE: If Yes, repeat ====Ransomware Payment Details==)
1742	N. [Op] + [FISMA Req] Do you have any other information regarding the
1743	ransomware incident not previously provided (e.g., communications with the
1744	threat actors, transcripts, audio recordings, emails, chats)? (Yes/No)
1745	1. Describe (DESIGN NOTE: If Yes: Open text)
1746	Incident Stage (I/D): Tactics, Techniques and Procedures
1747	(TTPs) and Indicators of Compromise (IOCs) Observed
1748	45. [RA] Would you like to document the tactics, techniques, and procedures (TTPs) and
1749	related indicators of compromise(s) (IOCs) you observed by using our offline
1750	template and uploading the completed file, or would you prefer to proceed and enter
1751	the TTPs and IOCs directly in this online form?
1752	(DESIGN NOTE: select one) (DESIGN NOTE: If "Template" is selected, skip over following questions 47,
1753	48, 49, 50).
1754	A. [] I'd like to use the offline template (DESIGN NOTE: If selected, proceed to Q47)
1755	B. [] I'd like to proceed with this report using the online form (DESIGN NOTE: If
1756	selected proceed to Q48)
1757	46. {Conditional on Q46.A is selected} [Op] You have indicated you will use the offline
1758	template to document your TTPs and IOCs, then will upload the file once complete.
1759	Please proceed with the download of the template and instructions (below) and return
1760	to this point in the online form to upload your completed file.
1761	A. Download the TTP/IOC template/instructions here: DOWNLOAD
1762	TEMPLATE/INSTRUCTIONS
1763	B. Upload the completed TTP/IOC file offline template here: UPLOAD
1764	TEMPLATE
1765	1. Select here to continue this report and return to upload your offline form
1766	later.
1767	
1768	Incident Stage (I/D): Tactics, Techniques and Procedures
1769	(TTPs) Observed
1770	47. {Conditional on Q46.B is selected} + [RA] You have indicated you want to
1771	document your TTPs and IOCs directly into this form. At this time, can you provide
1772	information regarding the TTPs the adversary leveraged as part of this incident?
1773	(Yes/No) (DESIGN NOTE: If No: DISPLAY NOTE: When, during your investigation, you discover
1774	knowledge about TTPs contributing to the incident, please return to this question and document them. If
1775	you have already documented and IOCs, you must also return to that section and provide the connections
1776	between the IOCs and TTPs documented that have factored into the incident.)

1777	48. {Conditional}[RC] (DESIGN NOTE: Question applies only if "Yes" to TTPs to report selection of
1778	"Proceed directly in report" to documenting TTP/IOC in Q46.B) You have indicated you have
1779	TTP(s) to report and would like to document those TTP(s) and related IOC(s) directly
1780	in this online form. Therefore, please begin by selecting the type(s) of networks 46 and
1781	systems the TTPs were observed within. (Select all that apply). []
1782	Enterprise/Traditional IT; [] Operational Technology/Industrial Control Systems; []
1783	Mobile Systems (DESIGN NOTE: Multi select)
1784	A. Are you familiar with the MITRE ATT&CK TTP framework? (Yes/No)
1785	
1786	B. Would you like to use CISA's internal tool to help you understand what TTPs you
1787	experienced? (Yes/No)
1788	1. (DESIGN NOTE: If Yes AND if No to "familiar with MITRE ATT&CK") Once you have
1789	completed using CISA's internal tool to help understand your TTPs, are you
1790	now able to use MITRE ATT&CK framework to identify your TTPs?
1791	(Yes/No)
1792	
1793	C. (DESIGN NOTE: If Yes to "familiar with the MITRE ATT&CK" {Conditional} [Op] +
1794	[FISMA Req] Select the appropriate MITRE ATT&CK tactics and/or
1795	technique(s) observed from the matrix associated with the network(s) you have
1796	selected
1797	1. One or more TTPs observed in this incident are not identified in MITRE
1798	ATT&CK, therefore we need to document those TTPs in a different method.
1799	[ ] Select if applicable (DESIGN NOTE: If selected allow for a combination of both
1800	MITRE ATT&CK TTP and alternate narrative method TTP identifications)
1801	

<sup>46</sup> 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.



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

Enterprise Networks	Mobile Networks	Industrial Control 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
Command and Control	Impact (physically to data/systems)	Impact (physically to data/systems)
Exfiltration		
Impact (physically to		
data/systems)		

1816 1817	i. Please provide a description and details of the TTPs observed in the category(ies) you have documented (DESIGN NOTE: Open text box)
1818	Incident Stage (I/D): Indicators of Compromise (IOCs) and
1819	associated Detection Methods Used
1820 1821 1822	(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.)
1823	49. [C-15] [RA] Do you have any Indicators of Compromise (IOCs) you can share with
1824	us? (Yes/No) (DISPLAY NOTE: You will be given an opportunity to associate reported IOC(s) with
1825	your entity's documented TTP(s) in a future step. (DESIGN NOTE: IF No: SKIP to Q52, the "Incident
1826	Stage (I/D): Malware Artifacts and Detection Logics/Analytics" section)
1827	(DESIGN NOTE: If Yes) There are two methods by which you can share IOCs with us.
1828	Option one is via a "copy/paste" of your IOC(s) into this form with opportunities to
1829	add additional IOC attributes once the system processes your "copy/paste". Option
1830	two is via providing the IOC(s) individually in a structured format wherein you
1831	provide attribute details and TTP mapping at the time of entry. (DISPLAY NOTE: Based
1832	on previous incident reporting and our experience, if there are 10 or fewer IOCs to report, the structured
1833	"individual build" approach may be the best option to document the IOCs.) Which method do you
1834	want to use to document your IOC(s)? [] "Copy/paste; [] "Individual build"
1835	
1836	1. [RC] (DISPLAY NOTE: To ensure we can ingest your data correctly you will need to provide
1837	your IOCs separated by a space, comma, semicolon, or new line.) Provide your IOC(s) via
1838	copy/paste here (DESIGN NOTE: Open text box)
1839	a. Upload via copy/paste method
1840	IOC Relation; Type; Context, Timeline [Start, Stop, Still ongoing (Y/N)]; IOC
1841	location observed
1842	1. Please validate and edit any errors to your IOC(s) here
1843	2. Based on the current IOC list reported, it is very helpful to
1844	CISA if you can provide additional context on the IOCs. The
1845	context which is particularly valuable to us is an explanation
1846	of whether the indicator is from the attacker, benign,
1847	unknown, the times seen, if the IOC is currently active in your
1848	environment, and the location the IOC was operating from
1849	within your network(s). It is preferred to have the attributes
1850	associated per individual IOC. At a minimum, the attributes
1851	can be applied to all IOCs of the same type. At what level are
1852	you able to provide us context on the IOC(s) you are sharing?
1853	[] Attributes per IOC entry [] Attributes per IOC type (Select
1854	one) (DESIGN NOTE: Single select)
1855	3. Based on the IOC(s) added to your report, please provide the
1856	overall IOC attributes as necessary:

1857	i.	Were th	nese IOCs [ ]Attacker, [ ]Benign, [ ]Unknown
1858		(Select	all that apply) (DESIGN NOTE: multi select)
1859	ii.	Please 1	provide the timeline of the IOC(s) collected
1860		1. Firs	st known time IOC operational in your
1861		env	ironment
1862		<b>2.</b> Is the	ne IOC still active in your environment? (Y/N)
1863		(DES	SIGN NOTE: If No)
1864		i.	Time IOC ceased operation within your
1865			environment
1866	iii.	Please s	select (one) the most severe location any of the
1867		IOCs w	vere operating from within your environment from
1868		this list	
1869		i.	Business demilitarized zone (DMZ) (Activity
1870			was observed in the business network's
1871			demilitarized zone (DMZ))
1872		ii.	Business network (Activity was observed in the
1873			business or corporate network of the entity;
1874			these systems would include corporate user
1875			workstations, application servers, and other non
1876			core management systems)
1877		iii.	Business network management (Activity was
1878			observed in business network management
1879			systems such as administrative user
1880			workstations, active directory servers, or other
1881			trust stores)
1882		iv.	Critical system. <sup>47</sup> DMZ (Activity was observed
1883			in the DMZ that exists between the business
1884			network and a critical system network. These
1885			systems may be internally facing services such
1886			as SharePoint sites, financial systems, or relay
1887			"jump" boxes into more critical systems.)
1888		v.	Critical system management (Activity was
1889			observed in high-level critical systems
1890			management such as human-machine interfaces
1891			in Industrial Control Systems)
- J <b></b>			<i></i>

<sup>&</sup>lt;sup>47</sup> **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 <a href="https://www.dhs.gov/publication/dhs-lexicon">https://www.dhs.gov/publication/dhs-lexicon</a>

1892	vi. Critical systems (Activity was observed in the
1893	critical systems that operate critical processes.)
1894	vii. Unknown
1895	viii. Other [describe] (DESIGN NOTE: Open Text)
1896	4. Based on each of the IOCs added to your report, please
1897	provide the individual IOC attributes as necessary
1898	i. Was the IOC [ ]Attacker, [ ]Benign, [ ]Unknown (Select
1899	one) (DESIGN NOTE: Single select)
1900	ii. Please provide the timeline of the IOC provided
1901	1. First known time IOC operational in your
1902	environment
1903	2. Is the IOC still active in your environment? (Y/N)
1904	(DESIGN NOTE: If No)
1905	i. Time IOC ceased operation within your
1906	environment
1907	iii. Please indicate any of these areas or locations in your
1908	organization's network(s) where you observed the IOC
1909	(select all that apply)
1910	1. Business demilitarized zone (Activity was observed
1911	in the business network's demilitarized zone [DMZ])
1912	2. Business network (Activity was observed in the
1913	business or corporate network of the entity; these
1914	systems would include corporate user workstations,
1915	application servers, and other non-core management
1916	systems)
1917	3. Business network management (Activity was
1918	observed in business network management systems
1919	such as administrative user workstations, active
1920	directory servers, or other trust stores)
1921	4. Critical system. 48 DMZ (Activity was observed in the
1922	DMZ that exists between the business network and a
1923	critical system network. These systems may be
1924	internally facing services such as SharePoint sites,
1925	financial systems, or relay "jump" boxes into more
1926	critical systems.)

<sup>&</sup>lt;sup>48</sup> **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 <a href="https://www.dhs.gov/publication/dhs-lexicon">https://www.dhs.gov/publication/dhs-lexicon</a>

1927	5. Critical system management (Activity was observed
1928	in high-level critical systems management such as
1929	human-machine interfaces in Industrial Control
1930	Systems)
1931	6. Critical systems (Activity was observed in the critical
1932	systems that operate critical processes.)
1933	7. Unknown
1934	8. Other [describe] (DESIGN NOTE: Open Text)
1935	b. Please associate the IOC(s) you provided with the appropriate
1936	TTP(s) you have already documented. If you have not yet
1937	documented any TTPs, please select [here] to omit this step for
1938	now. (DESIGN NOTE: if reporter selects "[here]" allow the IOC to TTP mapping
1939 1940	process to be postponed and DISPLAY NOTE: When, during your investigation, you discover knowledge about TTPs contributing to the incident and have
1940 1941	documented them, please return to this question and provide the associations
1942	between the IOCs and TTPs documented that have factored into the incident)
1943	2. Individual build method (DESIGN NOTE: For Data marking: reporter needs the
1944	opportunity to label the following IOC information as proprietary at some point, e.g., through
1945	data markings/options to be marked in the CISA 2015 section.)
1946	a. Please select the TTP with which these IOCs are associated.
1947	(DESIGN NOTE: if reporter selects "[here]" allow the IOC to TTP mapping
1948	process to be postponed and DISPLAY NOTE: When, during your investigation,
1949	you discover knowledge about TTPs contributing to the incident and have
1950	documented them, please return to this question and provide the associations
1951 1952	between the IOCs and TTPs documented that have factored into the incident.) (DESIGN NOTE: Select from TTP entered "pick-list" and allow reporter to
1953	associate the IOC with a TTP.)
1954	(=====DESIGN NOTE: This section is repeated for each type of IOC the
1955	reporter is providing =====)
1956	b. [Op] + [RR] What is the IOC's relation to the incident? (Attacker,
1957	Benign, Unknown) ((DESIGN NOTE: Select one)
1958	c. [C-15] [Op] + [RR] Select type of indicator of compromise (Select
1959	from list:):
1960	1. Autonomous System(s) (AS)
1961	2. Domain Name(s)
1962	3. Email Address(es)
1963	4. Email Message(s) (DESIGN NOTE: Allow option to upload Email
1964	Headers separate from Email Body.)
1965	5. IPv4 Address(es)
1966	6. IPv6 Address (es)
1967	7. Network Traffic
1968	8. URL
1969	9. File System Directory(ies)
1970	10. File Metadata

1971		11. Hash(es)
1972		12. Mutex(es)
1973		13. Software Metadata
1974		14. System Process(es)
1975		15. User Account(s)
1976		16. Windows Registry
1977		17. X.509 Certificate(s)
1978	d.	[C-15] + [RA] Please share any relevant context regarding these
1979		IOCs (DESIGN NOTE: Open text)
1980	e.	[Op] + [RR] Please enter your IOC timeline here
1981		1. First known time IOC operational in your environment
1982		2. Is the IOC still active in your environment? (Y/N) (DESIGN
1983		NOTE: If No)
1984		i. Time IOC ceased operation within your environment
1985	f.	[C-15] + [Op] + [RR] Please indicate any of these areas or
1986		locations in your organization's network(s) where you observed
1987		the IOC (select all that apply)
1988		
1989		i. Business demilitarized zone (Activity was observed in th
1990		business network's demilitarized zone [DMZ])
1991		ii. Business network (Activity was observed in the business
1992		or corporate network of the entity; these systems would
1993		include corporate user workstations, application servers,
1994		and other non-core management systems)
1995		iii. Business network management (Activity was observed in
1996		business network management systems such as
1997		administrative user workstations, active directory servers
1998		or other trust stores)
1999		iv. Critical system <sup>49</sup> DMZ (Activity was observed in the
2000		DMZ that exists between the business network and a
2001		critical system network. These systems may be internally
2002		facing services such as SharePoint sites, financial
2003		systems, or relay "jump" boxes into more critical
2004		systems.)
		-

<sup>&</sup>lt;sup>49</sup> **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 <a href="https://www.dhs.gov/publication/dhs-lexicon">https://www.dhs.gov/publication/dhs-lexicon</a>

2005	v.	Critical system management (Activity was observed in
2006		high-level critical systems management such as human-
2007		machine interfaces in Industrial Control Systems)
2008	vi.	Critical systems (Activity was observed in the critical
2009		systems that operate critical processes.)
2010	vii.	Unknown
2011	viii.	Other [describe] (DESIGN NOTE: Open Text)
2012	Indicator of Compromi	ise (IOC) Individual Data Marking
2013	50. [RR except FISMA do not	show] Should the IOC(s) and associated detail you have
2014	provided in this section be	considered commercial, financial, and proprietary under
2015	the Cybersecurity Informat	tion Sharing Act of 2015? [Yes/No]
2016	Incident Stage (I/D): In	ndicators of Compromise (IOCs): Detection
2017	Methods	
2018	51. [Op] + [RR] MITRE's D31	FEND matrix categorizes countermeasures into multiple
2019	categories. Detection action	ns are identified in the "Model" and "Detect" categories.
2020	Are you familiar with, and	or would you like to use MITRE D3FEND matrix to
2021	document your detection n	nethods? (Yes/No)
2022	a. (DESIGN NOTE: If y	es) Please select the detection methods you used to discover
2023	each observed act	tivity IOC using the MITRE D3FEND matrix (DISPLAY
2024		to this section at any point during the life cycle of this incident to
2025	document any addition	and detection methods used to help resolve this incident)

					А		raph of cyb	END ersecurity cour		3					
ATT&CK Look	cup					Se	arch D3FEND	's 620 Artifacts					D3FE	ND Looku	p
-	М	odel		Harden	-			Detect	<u> </u>			Isolate	Deceive	Evict	Restore
Asset Inventory	Network Mapping	Operational Activity Mapping	System Mapping	+	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	+	+	+	٠
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	Active	Operational			Emulated	Identifier	Analysis	Analysis			-				
Image Analysis	Logical Link Mapping	Dependency Mapping	Service Dependency Mapping		File Analysis	Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Behavior Analysis	File Access Pattern Analysis	Authorization Event Thresholding				
Configuration Inventory	Passive Logical	Operational Risk Assessment	System Dependency Mapping		File Content Analysis	Identifier Reputation Analysis	Allalysis	Certificate Analysis	Firmware Embedded Monitoring	Indirect Branch Call Analysis	Credential Compromise Scope				
Data Inventory	Link Mapping	Organization			File Content	Domain Name		Active	Code	-	Analysis				
Hardware	Network Traffic	Mapping	System Vulnerability Assessment		Rules	Reputation Analysis		Certificate Analysis	Firmware Verification	Process Code Segment Verification	Domain Account Monitoring				
Component Inventory	Policy Mapping				File Hashing	File Hash Reputation Analysis		Passive Certificate Analysis	Peripheral Firmware Verification	Process Self-	Job Function Access				
Network Node Inventory	Physical Link Mapping					IP Reputation		Client-server Payload	System	Modification Detection	Pattern Analysis				
Software Inventory	Active Physical					Analysis		Profiling	Firmware Verification	Process Spawn	Local Account Monitoring				
	Link Mapping					URL Reputation Analysis		Connection Attempt Analysis	Operating System Monitoring	Analysis	Resource Access				
						URL Analysis		DNS Traffic Analysis	Endpoint Health	Lineage Analysis	Pattern Analysis				
								File Carving	Beacon	Script Execution Analysis	Session Duration Analysis				
								Inbound Session Volume Analysis	Device Analysis Memory	Shadow Stack Comparisons	User Data Transfer Analysis				
								IPC Traffic Analysis	Boundary Tracking Scheduled	System Call Analysis	User Geolocation				
								Network Traffic	Job Analysis	File Creation	Logon Pattern Analysis				
								Community Deviation	System Daemon Monitoring	Analysis	Web Session Activity Analysis				
								Per Host Download- Upload Ratio Analysis	System File Analysis						
								Protocol Metadata Anomaly Detection	Service Binary Verification						
								Relay Pattern Analysis	System Init Config Analysis						

2026

2027

2028

2029

2030 2031

2032

2033

2034 2035

2036

2037

2038

2039 2040

2041

2042

b. (DESIGN NOTE: If No) (DESIGN NOTE: Multi select)

- 1. Did your organization choose a detection technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No)
  - I. (DESIGN NOTE: If Yes):
    - 1. Which tactic did your action fall under?
      - a. Model
        - 1. Asset inventory
        - 2. Network mapping
        - 3. Operational activity mapping
        - 4. System mapping
      - b. Detect
        - 1. File analysis
        - 2. Identifier analysis
        - 3. Message analysis
        - 4. Network traffic analysis

2043	5. Platform monitoring
2044	6. Process analysis
2045	7. User behavior analysis
2046	8. Description (DESIGN NOTE: Open text)
2047	II. (DESIGN NOTE: If No) If your organization is unable to use MITRE
2048	D3FEND, did not use any of the MITRE D3FEND detection
2049	methods, or is unsure which MITRE D3FEND detection method
2050	applies, select from the set of common detection methods below:
2051	1. Administrator
2052	2. Antivirus software
2053	3. Commercial and/or publicly available solution
2054	4. External source notification
2055	5. Human review
2056	6. Internally developed/proprietary solution
2057	7. Intrusion detection system (IDS)
2058	8. Log review
2059	9. User
2060	10. Unknown
2061	11. Other
2062	a. Please provide a description of the detection
2063	method(s). (DESIGN NOTE: Open text)
2064	Incident Stage (I/D): Malware Artifacts and Detection
2065	Logics/Analytics
2066	52. [C-15] [RA] Did you detect malicious software (malware) or scripts? (Yes/No)
2067	A. {Conditional} [Op] + [RR] (DESIGN NOTE: If Yes) Do you have any malware you
2068	can share with us? (Yes/No) (DESIGN NOTE: If Yes) Please upload here
2069	B. [C-15] {Conditional} [Op] + [RR] (DESIGN NOTE: If Yes) Please provide any
2070	additional detail or context regarding the malware you have shared with us
2071	(DESIGN NOTE: Open text)
2072	
2073	53. [Op] + [RR] Did you create any signatures or other detection analytics to identify
2074	and/or detect the threat activity you have reported? (Yes/No)
2075	{Conditional} [Op] + [RR] (DESIGN NOTE: If Yes)
2076	A. For each entry, please provide the following
2077	1. Description
2078	2. Pattern or rule
2079	3. Pattern or rule language or technology used (Yara, Snort, SIGMA, etc.)

2080	Incident Stage (I/D): Malware Artifacts and Detection
2081	Logics/Analytics: Data Classification Markings
2082	54. [CUI] [Op] + [RR] The default data marking for the malware artifacts and detection
2083	logic/analytics just reported is {insert default data marking here, default data marking
2084	is TBD). Would you like to change the default data marking? (Yes/No) (DISPLAY
2085	NOTE: The default marking with the lowest restriction available will be applied to fields not previously
2086	entered with a data marking label automatically to all submissions in the Malware Artifacts and Detection
2087	Logics/Analytics sub-section. Although you will be given an opportunity to change the markings for
2088	responses to individual questions.)  (Conditional) [Onl   [DD] approximation responses to a february data manking a best
2089	{Conditional} [Op] + [RR] (DESIGN NOTE: If Yes) Which of these data markings best
2090 2091	describe your malware artifacts and detection logics/analytics?
2091	(DESIGN NOTE: See Appendix 1 for options.)
2092	Incident Stage (I/D): Data Sources Used and Attribution
2093	Data Sources Used
2094	55. [Op] + [RR] Were external data sources such as data from threat
2095	information/intelligence reporting used to discover or aid in discovering this incident's
2096	(Yes/No)
2097	[If Yes]Provide the following for each data source
2098	A. [Op] + [FISMA Req] Report title and number (if applicable)
2099	1. Name/description of data source (can include author, company providing the
2100	data source, or general description)
2101	2. Link to report/data source (if applicable and available to share)
2102	Attribution
2103	56. [RA] Have you attributed this incident to a threat actor? (Yes/No, This incident is
2104	currently an unattributed cyber intrusion/Maybe)
2105	{Conditional} [Op] (DESIGN NOTE: If Yes or Maybe) Provide the name of the "threat
2106	actor" and the source used to support this assessment below
2107	[] The attributed threat actor name and/or attribution source is classified (select if
2108	true)
2109 2110	DISPLAY NOTE: If you used a classified source to help in your attribution, do not complete the following
2110	You will be contacted via a secure means to discuss further if necessary)  A. Threat actor name (could be name of advanced persistent threat [APT] actor,
2112	ransomware group, etc.) (DESIGN NOTE: Open text)
2113	B. Was this attribution claim based on one of the data sources you previously
2114	provided? (DESIGN NOTE: Allow to select from list (one to many entries.))
2115	If not, please provide the attribution source(s) (DESIGN NOTE: One to many
2116	entries.)
2117	1. Name of attribution source(s) (DESIGN NOTE one to many entries.)
2118	2. URL/Web link to validate source material (DESIGN NOTE: One to many
2119	entries.) (DESIGN NOTE: Open text)
2120	3. Report title(s) and number(s) (if applicable) (DESIGN NOTE: One to many
2121	entries) (DESIGN NOTE: Open text)

2122	4. Other details (DESIGN NOTE: One to many entries.) (DESIGN NOTE: Open text)
2123	C. What is your level of confidence. <sup>50</sup> in your attribution (DESIGN NOTE: Select one)
2124	1. Confirmed by other sources: confirmed by other independent sources; logical
2125	in itself; consistent with other information on the subject
2126	2. Probably true: not confirmed; logical in itself; consistent with other
2127	information on the subject
2128	3. Possibly true: not confirmed; reasonably logical in itself; agrees with some
2129	other information on the subject
2130	D. Provide any additional information you feel is relevant (DESIGN NOTE: Open text)
2131	
2132	{Conditional} [Op] + [RR] (DESIGN NOTE: If No) This incident is currently an
2133	unattributed cyber intrusion. Please provide any additional information you feel is
2134	relevant and will aid in attribution. (DESIGN NOTE: Open text)
2135	m. Assistance
2136	Assistance from CISA
2137	57. [Op] + [RR] Are you interested in receiving incident response assistance from CISA
2138	to the extent available? (Yes/No)
2139	58. [Op] + [RR] Are you interested in additional collaboration or information sharing
2140	with CISA around this incident to the extent feasible? (Yes/No)
2141	Third Party Assistance
2142	59. [Op] + [RR] Are you utilizing an external third party to provide assistance with the
2143	reported incident? (Yes/No)
2144	A. (DESIGN NOTE: If Yes) Provide the name of third-party entity(ies) (DESIGN NOTE: Open
2145	text)
2146	Data Sharing and Logging Readiness
2147	60. [OP] + [RR] Are you willing to share the results of third-party analysis with CISA?
2148	(Yes/No) (DESIGN NOTE: Only Display if "Yes" to "third party" question prior.)
2149	61. [OP] + [RR] Are you willing to share data (such as logs or other technical artifacts)
2150	about this incident with CISA? (Yes/No)
2151	1. {Conditional} [Op] + [FISMA Req] [If Yes] Please select all categories of
2152	data (such as logs or other technical artifacts) you are willing to provide. If
2153	necessary, our request for logs and technical artifacts would encompass only
2154	information related to the incident (DESIGN NOTE: Multi select) (DISPLAY NOTE:
2155	You are not being asked to share this data with CISA at this time/through this report. The
2156 2157	purpose of this question is for CISA to understand the extent to which such data exists, and you are willing to share it with CISA for potential analysis.)
2158	a. Identity-based logs for the following

50 https://www.misp-project.org/taxonomies.html#\_admiralty\_scale https://www.threat-intelligence.eu/methodologies/

2159	1. Identity and credential management
2160	2. Privileged identity and credential management
2161	3. Authentication and authorization
2162	4. User accounts and user account meta-data
2163	b. Network
2164	1. Email filtering, spam, and phishing logs
2165	2. Network device infrastructure logs (for devices with multiple
2166	interfaces: interface MAC if correlated to the De-NAT IP
2167	address)
2168	3. Network device infrastructure logs (e.g., general logging,
2169	access, authorization, and accounting)
2170	4. Data loss prevention logs
2171	5. Network traffic (e.g., packet capture) artifacts
2172	6. Network traffic (e.g., Netflow, Enhanced Netflow, Zeek Logs,
2173	etc.) artifacts
2174	c. Host:
2175	1. Operating systems (e.g., Windows infrastructure and
2176	operating systems, MacOS, BSD)
2177	2. PKI and other multifactor applications and infrastructure
2178	3. Antivirus and behavior-based malware protection
2179	4. Other host logs (e.g., operating system, database logs,
2180	application logs)
2181	d. Vulnerability
2182	1. Vulnerability assessments
2183	2. Penetration test results
2184	e. Mobile
2185	1. Mobile (phones and tablets) EMM (UEM) / MTD server logs
2186	2. Mobile (phones and tablets) EMM (UEM) / MTD agent logs
2187	f. Containers:
2188	1. Container (e.g., supply chain, image, engine
2189	(MGT/orchestration, OS, cluster/pod events)
2190	g. Cloud unique data not specified above
2191	1. Cloud environments (general events and general logging)
2192	2. System configuration and performance
2193	3. Virtualization systems
2194	h. Mainframes
2195	1. Mainframe unique logging not covered above
2196	i. Communications

2197	1. Any communications with the threat actors (either by the
2198	entity or another entity on behalf of the entity) (e.g., emails
2199	[with full headers and attachments], chats, etc.)
2200	2. Notes, transcripts, and audio recordings of any
2201	communications with threat actors
2202	j. Financial
2203	1. Any log files supporting financial records and accounts
2204	associated with the incident (DISPLAY NOTE: This is not intended to
2205	include actual financial account information, e.g., account numbers, etc.)
2206	k. Forensic images:
2207	1. Forensic images (e.g., full disk, system, volume etc.) relevant
2208	to the incident
2209	2. Memory images relevant to the incident
2210	1. Malicious code
2211	1. Malicious code and associated files related to the incident
2212	m. Exfiltrated data
2213	1. Data and metadata exfiltrated related to the incident (DISPLAY
2214	NOTE: This is not intended to include actual compromised data.)
2215	2. Evidence of data and metadata exfiltrated, related to the
2216	incident
2217	n. Reporting
2218	1. Forensic and other reporting related to or concerning the
2219	incident (internal or external party originated)
2220	
2221	n. Analysis (A) Stage <sup>51</sup>
2222	62. [RA] Have you begun the analysis stage? (Yes/No/Unsure) (DISPLAY Note: The focus in
2223	this stage is on analyzing the incident in more detail, determining the root cause, and assessing the impact.)
2224	A. (DESIGN NOTE: If Yes) Please provide the date (yyyy-mm-dd) you began the analysis
2225	stage
2226	63. [FISMA Req] Has the suspicious activity been declared an incident? (Yes/No)
2227	(DISPLAY NOTE: This event and time is different from the first time of incident detection. An incident
2228 2229	declaration is the point when your organization has officially analyzed the information and determined the activity detected is, in fact, evidence of a cyber incident.)
2230	A. (DESIGN NOTE: If Yes) Provide date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
2230	offset>) the incident was declared
<b></b>	offser j the metaent was declared

<sup>&</sup>lt;sup>51</sup> 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 <a href="https://www.dhs.gov/publication/dhs-lexicon">https://www.dhs.gov/publication/dhs-lexicon</a>]

2232	Incident Stage (A): Impacted Users and Systems
2233	
2234	64. [RA] Please identify the impacted users (number of impacted privileged and/or
2235	standard information technology (IT) users) (DISPLAY NOTE: This is not necessarily all users,
2236	but those users impacted by activity during the incident.) (DESIGN NOTE: Multi select then quantity
2237	entered.)
2238	A. Privileged/system/administrative/service-level IT user quantity impacted (DESIGN
2239	NOTE: Quantity)
2240	1. [Op] How are these users impacted (e.g., accounts locked, removed, other)?
2241	B. Standard IT user quantity impacted (DESIGN NOTE: Quantity)
2242	1. [Op] How are these users impacted (e.g., accounts locked, removed, other)?
2243	65. [C-15] [RA] With respect to information systems you own and/or operate that are
2244	impacted by or involved in this incident: (DESIGN NOTE: These set of questions repeat for
2245	every "instance" of Impacted Systems identified below.)
2246	A. [FISMA Req] + [FedRAMP] Please identify whether any impacted information
2247	system, network, and/or device supports any elements of the intelligence
2248	community or contains information that has been determined by the United States
2249	Government pursuant to an Executive Order or statute to require protection
2250	against unauthorized disclosure for reasons of national defense or foreign
2251	relations, or any restricted data, as defined in 42 U.S.C. 2014(y) (Yes/No).
2252	1. (DESIGN NOTE: If Yes) Please identify the relevant federal entity category
2253	(DESIGN NOTE: Multi select)
2254	a. Federal civilian executive branch (FCEB) - FISMA System
2255	(Yes/No)
2256	b. Intelligence community (Yes/No)
2257	c. Federal judicial branch (Yes/No)
2258	d. Federal legislative branch (Yes/No)
2259	e. DOD system, program, or platform (Yes/No)
2260	B. {Conditional} (DESIGN NOTE: Conditional to "Yes" selection to "A.1.a. Federal Civilian
2261	Executive Branch (FCEB) - FISMA System (Yes/No)". If Yes)
2262	1. [FISMA Req] Please provide the FISMA system name
2263	2. [FISMA Req] Please select the type of FISMA system
2264	a. General support system
2265	b. Major application
2266	c. Other
2267	1. Please provide the system type (DESIGN NOTE: Open text)
2268	3. [CUI] [FISMA Req] Contact information of the federal employee identified
2269	as the system owner
2270	a. Name
2271	1. First
2271	2. Last
4414	Z. Last

2273	b. Phone number(s)
2274	1. Unclassified
2275	2. [Op]Classified
2276	c. Email address(es)
2277	1. Unclassified
2278	2. [Op]Classified
2279	d. Position or title
2280	C. [C-15] [RA] Identify and describe the function of each individual (or group of
2281	similar) affected network(s), device(s), and/or Information System(s), specifically
2282	with respect to the category, system type, services provided, name, location and
2283	government customer communities supported
2284	1. Category (Select all that apply) (DESIGN NOTE: Multi select)
2285	a. []Enterprise networks or systems <sup>52</sup> : Impacted [confirmed]
2286	[suspected] (Select one) (DESIGN NOTE: Single select)
2287	b. []Operational technology. <sup>53</sup> and industrial control systems:
2288	Impacted [confirmed] [suspected] (Select one) (DESIGN NOTE: Single
2289	select)
2290	c. []Mobile devices <sup>54</sup> : Impacted [confirmed] [suspected] (Select
2291	one) (DESIGN NOTE: Single select)
2292	
2293	2. Systems type (DESIGN NOTE: Multi select then quantity entered)
2294	a. Endpoint devices (non-server devices)
2295	1. Authentication token or device
2296	i. Operating systems (OS) (DESIGN NOTE: 1.i.,ii.,iii and 2.,
2297	repeated for each option selected)
2298	<ul><li>i. OS name(s)</li><li>ii. OS version number(s)</li></ul>
2299	
2300	
2301	2. Desktop
2302	3. Laptop  A. Madia (a.g. baskyn tanas diek madia (a.g. CDa DVDa)
2303	4. Media (e.g., backup tapes, disk media (e.g., CDs, DVDs), documents, flash drive or card, hard disk drive, media player,
2304	
2305	recorder)

<sup>&</sup>lt;sup>52</sup> 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.

<sup>&</sup>lt;sup>53</sup> 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.

2306		5. Mobile phone or smartphone
2307		6. Peripheral (e.g., printer, copier, fax, identity smart card,
2308		payment card (such as a magstripe or EMV))
2309		7. Point of sale (POS) terminal
2310		8. Tablet
2311		9. Telephone
2312		•
		10. Voice over Internet Protocol (VoIP) phone 11. Other/unknown (DESIGN NOTE: Open text)
<ul><li>2313</li><li>2314</li></ul>	b.	Server types
	0.	1. Active Directory (AD) Components
2315		
2316 2317		i. Operating systems (OS) (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)
2318		i. OS name(s)
2319		ii. OS version number(s)
2320		iii. Number impacted of each OS version
2321		2. Certificate Authority (CA)
2322		3. Domain Name System (DNS)
2323		4. Dynamic Host Configuration Protocol (DHCP)
2324		5. Email
2325		6. File
2326		7. File Transfer Protocol (FTP)
2327		8. Kerberos
2328		9. Lightweight Directory Access Protocol/Lightweight Directory
2329		Access Protocol over Secure Sockets Layer (LDAP/LDAP[S]
2330		10. Network Time Protocol (NTP)
2331		11. Print
2332		12. Remote log(s) (e.g., email, VPN, Syslog, R-Syslog, Syslog-
2333		NG)
2334		13. Remote Shell (RSH)
2335		14. Security Information and Event Management (SIEM)
2336		15. Secure Shell (SSH)
2337		16. TELNET
2338		17. Virtual Private Network (VPN)
2339		18. Web
2340		19. Voice over Internet Protocol (VoIP) Gateways
2341		20. Authentication, Authorization, and Accounting (AAA)
2342		Services (e.g., Radius, Terminal Access Controller Access-
2343		Control System [TACACS+])
2344		21. Operational (OT) and Open-Source Software (OSS) types
2345		(e.g., Apache HTTP Server)
2346		22. Other

2347	i. Please list the additional server type(s) (DESIGN NOTE:
2348	Open text)
2349	c. Network Devices
2350	1. Firewalls
2351	1. Operating systems (OS) (1.i, ii and iii. repeated for
2352	each selected)
2353	i. OS name(s)
2354	ii. OS version number(s)
2355	iii. Number impacted of each OS version
2356	2. Intrusion Detection System (IDS)
2357	3. Intrusion Protection System (IPS)
2358	4. Hub
2359	5. Load Balancers
2360	6. Proxies
2361	7. Routers
2362	8. Switches
2363	9. Other
2364	i. Please list the additional network device type(s) (DESIGN
2365	NOTE: Open text)
2366	d. Identity providers (IdP)
2367	1. Active Directory
2368	2. Active Directory Federation Services (ADFS)
2369	3. Amazon
2370	4. Azure Active Directory
2371	5. Facebook
2372	6. Google Workspace
2373	7. Lightweight Directory Access Protocol (LDAP)
2374	8. Login.gov
2375	9. Ping Federate
2376	10. OpenID Connect
2377	i. Provide the name of the provider(s) (DESIGN NOTE: Open
2378	text)
2379	11. Okta
2380	12. Security Assertion Markup Language (SAML)
2381	i. Provide the name of the provider(s) (DESIGN NOTE: Open
2382	text)
2383	13. Other identity providers
2384	i. Please provide the name of the identity provider(s)
2385	(DESIGN NOTE: Open text)
2386	3. Name of system(s) (DISPLAY NOTE: Provide name of system to add fidelity to the system
2387	(or group of systems) that is entered in this instance (e.g., clarifying names of servers.)) (DESIGN
2388	NOTE: Open text)

2389	4. Name of system(s) services provided (e.g., active directory, email, web,
2390	boundary firewall, key personnel mobile device) (DESIGN NOTE: Open text)
2391	5. Physical location(s) of system or group of systems
2392	a. [] Select if same as impacted facility address entered earlier
2393	b. If not the same address as impacted facility, then please provide
2394	address of impacted system(s)
2395	1. Street name and number
2396	2. City
2397	3. State
2398	4. Postal code
2399	5. Country
2400	6. Is the impact or involvement of the system (or group of systems) identified []
2401	confirmed or [] suspected at the time of report? (DESIGN NOTE: Select one.)
2402	
2403	D. [Op] + [RR] Is the system identified as part of the High Value Asset (HVA). 55
2404	Program (Yes/No)
2405	E. [Op] + [RR] Is the impacted system designated as a National Security System <sup>56</sup>
2406	(Yes/No)
2407	F. {Conditional}(DESIGN NOTE: Conditional to "Yes" selection to D. High Value Asset (HVA)
2408	Program (Yes/No).)
2409	1. What is the HVA Identification Number?
2410	2. For each HVA listed, what services does it provide?
2411	a. For each service, what communities does it support? (DESIGN NOTE:
2412	Open text)
2413	3. Does this HVA have connections to other HVAs? (Yes/No)
2414	a. (DESIGN NOTE: If Yes) Are these connections internal to the agency,
2415	external to the agency, or both? (Internal/External/Both)
2416	b. (DESIGN NOTE: If Yes) Do you know what the other HVAs are?
2417	(Yes/No)
2418	1. (DESIGN NOTE: If Yes) Please list the other HVA(s).
2419	i. For each HVA listed, what services does it provide?
2420	(DESIGN NOTE: Open text)
2421	1. For each service, what communities does it support?
2422	(DESIGN NOTE: Open text)
2423	2. Do you have contact information for the other HVA(s)?
2424	(Yes/No)
2425	i. [CUI] (DESIGN NOTE: If Yes)
2426	1. Name

<sup>55</sup> https://www.cisa.gov/resources-tools/programs/high-value-asset-program-management-office
56 NSS is defined in law here: 40 USC 11103: Applicability to national security systems (house.gov)
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

2427	i. First	
2428	ii. Last	
2429	2. Phone number(s)	
2430	i. Unclassified	
2431	ii. [Op]Classified	
2432	3. Email address(es)	
2433	i. Unclassified	
2434	ii. [Op]Classified	
2435	4. Position or title	
2436	5. Time zone	
2437 2438	Incident Stage (A): Initial Access "Patient Zero" Detail	1s
2439	$66. \{Conditional\}[Op] + [RR] $ (DESIGN NOTE: Executes if reporter has identified one	Initial Access
2440	or more TTPs observed above in the "Initial Access" category in any of the MITRE	10 techniques
2441	ATT&CK TTP matrices (example in "red box" to the right), this list is a "Dynamically	Content Injection
2442	created" list at time of question determined by which MITRE ATT&CK "Initial Access"  TTPs were selected.) You have observed and identified an "initial access"	Drive-by Compromise
2443		Exploit Public- Facing
2444	TTP. <sup>57</sup> in this incident. Have you identified the initially affected	Application
2445	endpoint, device, account, and/or application commonly referred to as	External Remote Services
2446	"patient zero"? (Yes/No) (DESIGN NOTE: If Yes, go to Q 69.)	Hardware Additions
2447 2448	67. {Conditional}[Op] + [RR] (DESIGN NOTE: Trigger this question if no MITRE	II Phishing (4)
2449	ATT&CK TTPs were entered to identify any Initial Access TTPs and the narrative response has been parsed into discrete TTPs to create a list.) Have you identified any	Replication Through
2450	initial access TTPs that you have attributed as the initial entry into your	Removable Media Supply Chain
2451	networks, commonly referred to as "patient zero"? (Yes /No) (DESIGN	Compromise (3)
2451	NOTE: If Yes, go to Q 69.)	Trusted Relationship
2453	68. {Conditional}[Op] + [RR] > [Triggered only if "Yes" from either Q67	Valid Accounts (4)
2454	or Q68] Please select from your reported initial access observed activity:	TP(s) and
2455	provide the technique used to gain the initial access to patient zero.	(-)
2456	A. (DESIGN NOTE: If Yes) Was the "patient zero" already entered with the re	st of the
2457	impacted systems? (Yes/No)	or or the
2458	1. (DESIGN NOTE: If Yes) Please select from your list of impacted systems.	ms the
2459	system(s) you believe to be "patient zero." (DESIGN NOTE: Allow to s	
2460	previously entered impacted system (from question highlighted in "red box" below	
		,

<sup>&</sup>lt;sup>57</sup> Tactics, Techniques and Procedures (TTP)

2461 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 every "instance" of Impacted Systems identified below.) A. [C-15][RA] Identify and describe the function of each individual (or group of similar) affected network(s), device(s), and/or Information System(s), specifically with respect to the category, system type, services provided, name location and government customer communities supported: 1. Category: a. Enterprise Networks or Systems<sup>47</sup>: Impacted [confirmed, b. Operational Technology<sup>48</sup> and Industrial Control Systems: Impacted [confirmed, suspected] c. Mobile Devices<sup>49</sup>: 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) 1. Authentication token or device Operating Systems (OS) (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected) i. OS name(s) ii. OS version number(s) iii. Number impacted of each OS version 2462 B. [C-15] (DESIGN NOTE: If "No" or the system was not found in preexisting list then:) If the 2463 system is not yet entered, please enter "patient zero" details now. 2464 1. Select the initial access system category and type (DESIGN NOTE: Follow same 2465 2466 format as in previous Impacted System entries. Pull from the list already identified in question 2467 "Please Identify Impacted System". If already entered, allow reporter to select the system as "Patient Zero", otherwise allow reporter to enter in Patient Zero system details in same format.) 2468 C. When was the date/time of initial access in this incident? 2469 1. Date and Time (yyyy-mm-dd HH:MM -<UTC offset>) 2470 2471 Incident Stage (A): Detailed Informational Impacts 2472 69. {Conditional}[FISMA Req + FedRAMP reporting only] (DESIGN NOTE: Display only if 2473 2474 "Classified data 'spillage' to unapproved networks" is selected in Incident Result. Reference "red box" 2475 [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) 2476 You indicated earlier that the incident resulted in spillage of classified information, 2477 please provide more details below (DISPLAY NOTE: DISCLAIMER Do NOT provide any 2478 2479 classified information in the following responses) A. What classification guide or source material was used to validate that the 2480 information spilled was classified? 2481 B. What was the root cause of the spillage? (DESIGN NOTE: Open text) 2482

2483	C. [CUI]Has an appeal or challenge been issued on the spillage of classified
2484	information? (Yes/No)
2485	1. On what date?
2486	2. [CUI]To whom was the appeal or challenge issued?
2487	3. Has the appeal been completed? (Yes/No)
2488	4. Was this appeal accepted or denied? (Accepted/Denied)
2489	a. If so, on what date was the appeal accepted or denied?
2490	
2491	(DESIGN NOTE: Execute this question if any impact is selected from the earlier Informational Impacts to
2492	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 impact <sup>36</sup> of this incident?  A. No impact B. Low impact C. Moderate impact D. High impact E. Critical impact (unrecoverable)
2493	F. Unknown
2494	70. {Conditional}[RC] Earlier in the form, you selected an informational impact <sup>58</sup> to
2495	your entity of (DESIGN NOTE: Place selected choice of Informational Impact question here, e.g., "High
2496	Impact"). We would like more details on your information impacts; can you please
2497	provide more details on any "suspected, but not confirmed" and/or "confirmed"
2498	known informational impact(s) from the incident?
2499	
2500	A. Please provide details on the "suspected" and/or "confirmed" informational
2501	impact(s) from this incident: (DESIGN NOTE: (Multi select)
2502	i. [] Suspected, but not yet confirmed
2503	1. Which of these information types do you suspect was impacted?
2504	(DESIGN NOTE: Multi select)
2505	a. Classified material (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option
2506	selected) (DESIGN NOTE: if these follow-on questions are same per info type
2507	selected, give option to copy over the same responses)
2508	1. How was the <u>suspected</u> information impact discovered?
2509	(Select all that apply)
2510	i. Some evidence of access but unclear evidence of
2511	exfiltration
2311	
2512	ii. Threat actor has provided inconclusive evidence of information impact (e.g., pictures of file directories)

<sup>&</sup>lt;sup>58</sup> **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>

2514	iii. Other inconclusive evidence of threat actor access/use of
2515	the information (please describe) (DESIGN NOTE: Open text if
2516	selected)
2517	iv. We were informed by an independent third party
2518	2. Was the system where the information was located a critical
2519	system. <sup>59</sup> ? (Yes/No)
2520	b. Communications (e.g., emails, instant messages)
2521	c. Administrative credentials
2522	d. User or other non-administrative credentials
2523	e. Financial
2524	f. Dissemination controlled
2525	1. Legal
2526	2. Proprietary
2527	3. Other personal information
2528	g. Defense information (as the information relates to unclassified
2529	cyber threat information/indicators (CTI), export controlled,
2530	operational security (OPSEC) and/or information)
2531	1. Unclassified CTI
2532	2. Export controlled information
2532 2533	3. OPSEC information
2534	3. Of SEC information
2535	ii. [] Confirmed
2536 2537	1. (DESIGN NOTE: If Yes) What type of information impact? (DESIGN NOTE: Select Privacy Data Breach and/or Other Data Compromise and/or Credential
2537 2538	Compromise) (DESIGN NOTE: Multi select)
2539	a. [] Privacy data breach (DESIGN NOTE: If Privacy data breach, then ask
2540	following) (DESIGN NOTE: Multi select)
2541	1. What type of information was impacted? (DESIGN NOTE: Multi
2542	select)
2543	i. Financial (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option
2544	selected)
2545	1. How was the information loss identified? (Select all
2546	that apply)
2547	i. The information was seen outside the authorized
2548	system (e.g., darkweb, leaksite, etc.) (DESIGN
2549	NOTE: Flagged as exploited)

<sup>&</sup>lt;sup>59</sup> **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 <a href="https://www.dhs.gov/publication/dhs-lexicon">https://www.dhs.gov/publication/dhs-lexicon</a>

2550	ii. The information was seen being exfiltrated from
2551	the authorized system and/or network (DESIGN
2552	NOTE: Flagged as loss)
2553	iii. We were informed by an independent third
2554	party (DESIGN NOTE: Flagged as loss)
2555	iv. Other evidence of threat actor access/use of the
2556	information (please describe) (Design Note: Open
2557	Text if selected)
2558	2. Was the system where the information was located a
2559	critical system? (Yes/No)
2560	ii. Dissemination Controlled
2561	1. Legal
2562	2. Proprietary
2563	3. Other personal information
2564	
2565	b. [] Other data compromise (DESIGN NOTE: If Other data compromise,
2566	then ask the following)
2567	1. What type of information was impacted? (DESIGN NOTE: Multi
2568	select)
2569	iii. Communications (DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for
2570	each option selected)
2571	1. How was the information loss identified
2572	i. The information was seen outside the authorized
2573	system. (e.g., darkweb, leaksite, etc.)
2574	ii. The information was seen being exfiltrated from
2575	the authorized system and/or network
2576	iii. We were informed by and independent third
2577	party
2578	iv. Other evidence of threat actor access/use of the
2579	information (please describe)
2580	2. Was the system where this information was located a
2581	critical system? (Yes/No)
2582	i. Dissemination controlled
2583	i. Proprietary
2584	ii. Classified
2585	iii. Defense information (as the information relates to
2586	unclassified cyber threat information/indicators (CTI),
2587	export controlled, OPSEC and/or information)
2588	i. CTI
2589	ii. Export controlled information
2590	iii. OPSEC information

2591	
2592	c. [] Credential compromise (DESIGN NOTE: If credential compromise, then
2593	ask the following)
2594	a. What types of credentials were compromised? (DESIGN
2595	NOTE: Multi select)
2596 2597	i. User or other non-administrative credentials (DESIGN NOTE: 1.i.,ii.,iii.,iv and 2., repeated for each option
2598	selected)
2599	1. How did you or others identify the compromise of
2600	the credentials? (Select all that apply)
2601	A. The information was seen outside the
2602	authorized system (e.g., darkweb, leaksite,
2603	etc.)
2604	B. The information was seen being
2605	exfiltrated from the authorized system
2606	and/or network
2607	C. We were informed by an
2608	independent third party
2609	D. Other evidence of threat actor
2610	access/use of the information (please
2611	describe) (DESIGN NOTE: Open Text if selected)
2612	2. Was the system where this information was
2613	located a critical system? (Yes/No)
2614	ii. Administrative credentials
2615	1. How was the compromise of the credentials
2616	identified? (DESIGN NOTE: Select all that apply)
2617	A. The information was seen outside the
2618	authorized system. (e.g., darkweb,
2619	leaksite, etc.)
2620	B. The information was seen being
2621	exfiltrated from the authorized system
2622	and/or network (DESIGN NOTE: Flagged as loss)
2623	C. We were informed by an
2624	independent third party (DESIGN NOTE:
2625	Flagged as loss)
2626	D. Other evidence of threat actor
2627	access/use of the information (please
2628	describe) (DESIGN NOTE: Open Text if selected)
2629	2. Was this credential on or did it have access to a
2630	critical system? (Yes/No)
2631	

2632	Incident Stage (A): Breach Details
2633	
2634	(DESIGN NOTE: Executes if incident is flagged as a Breach Incident in "Breach Severity Assessment"
2635	earlier as indicated in response to questions flagged in "red box" below:)
	[Op] + [FISMA Req] At this time, has the incident resulted in any confirmed
	unauthorized access to personally identifiable information? (Yes/No) (DESIGN NOTE: Ifl Yes, 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
	3. Unauthorized disclosure
	<ul> <li>4. Unauthorized acquisition</li> <li>B. Was the information accessed by (select all that apply):</li> </ul>
	1. A person other than an authorized user
	<ol> <li>An authorized user who accessed the record(s) for an other-than-authorized purpose</li> </ol>
2636	
	[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
	Access to personally identifiable information? (Yes/No) (DESIGN NOTE: If Yes, flag as  Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access
	the" and "accessed by" only if "Yes".)  A. Was the potential unauthorized access due to: (select all that apply)
	1. Loss of control
	Compromise     Unauthorized disclosure
	4. Unauthorized acquisition
	B. Was the information potentially accessed by: (select all that apply)
	<ol> <li>A person other than an authorized user</li> <li>An authorized user who accessed the information for an other-than-</li> </ol>
2637	authorized purpose
2638	71. {Conditional}[Op] + [FISMA Req] Earlier in this form, you provided the following
2639	description of this incident: (DESIGN NOTE: Pull forward the information entered by reporter
2640	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 incident 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
2641	network firewall, and a web server").)
2642	You have also previously indicated there was actual or potential unauthorized access
2643	to personally identifiable information (PII). Please add any available additional
2644	context on the PII that was impacted. However, DO NOT include samples of actual
2645	PII in this response.
2646	72. [FISMA Req] Did this incident involve a cyber- or non-cyber-related breach of PII?
2647	(DESIGN NOTE: Single-select)
2648	A. Cyber-related
2649	B. Non-cyber related (e.g., personnel information with PII found in a public
2650	dumpster)
2651	C. Both

2652	73. [FISMA Req] If you have any additional details regarding what has been observed or								
2653	identified with respect to the PII breach, please describe that here. However, DO								
2654	NOT include samples of actual PII in this response. (DESIGN NOTE: Open text)								
2655	Impacted Individuals								
2656	74. [FISMA Req] How many individuals' PII was impacted. 60?								
2657	75. [FISMA Req] Were affected individuals notified? (Yes/No/Pending)								
2658	A. (DESIGN NOTE: If Yes or Pending) How were (or will the) individuals (be) notified?								
2659	(Select all applicable)								
2660	1. Email								
2661	a. How many individuals were (or will be) notified using this								
2662	method?								
2663	2. Short message service (SMS)								
2664	a. How many individuals were (or will be) notified using this								
2665	method?								
2666	3. Verbal								
2667	a. How many individuals were (or will be) notified using this								
2668	method?								
2669	4. Parcel								
2670	a. How many individuals were (or will be) notified using this								
2671	method?								
2672	5. Other (Please list the method that was or will be used)								
2673	a. How many individuals were notified using this method?								
2674	76. [CUI] [FISMA Req] Were mitigation services in the form of monitoring, insurances								
2675	and/or counseling provided or offered to affected individuals? (Yes/No)								
2676	A. (DESIGN NOTE: If Yes) Which mitigation services have you made available to								
2677	impacted individuals? (Please select all that apply):								
2678	1. Identity monitoring								
2679	2. Credit monitoring								
2680	3. Identity theft insurance								
2681	4. Full-service identity counseling and remediation services								
2682	5. [CUI] Other (describe)								
2683	PII Accessed and/or Impacted								
2684	77. [FISMA Req] For each type of PII, provide how many records instances of a PII								
2685	category or type were accessed, potentially accessed, or otherwise impacted?								
2686	(DISPLAY NOTE: Use approximate counts if final counts are not available) (DESIGN NOTE: Multi select								
2687	for each PII "category" (e.g, Identifying numbers, Biographical Information, etc.) with the appropriate								
2688	"accessed or impacted flags".)								
2689	A. Personally Identifying Numbers (DESIGN NOTE: Multi select and for sub questions								
2690	"a., b., c.", repeated for each response selected)								

<sup>&</sup>lt;sup>60</sup> **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).

2691	1. Full social security number
2692	a. Provide count
2693	b. Is this count known or approximate? (Known/Approximate)
2694	c. Did potential or confirmed access occur? (Potential/Confirmed)
2695	2. Truncated or partial social security number
2696	3. Driver's license number
2697	4. License plate number
2698	5. Drug Enforcement Administration (DEA) registration number
2699	6. File/case identification (ID) number
2700	7. Patient ID number
2701	8. Health plan beneficiary number
2702	9. Student ID number
2703	10. Federal student aid number
2704	11. Passport number
2705	12. Alien registration number
2706	13. Department of Defense (DOD) ID number
2707	14. DOD benefits number
2708	15. Employee Identification Number
2709	16. Professional license number
2710	17. Taxpayer Identification Number
2711	18. Business Taxpayer Identification Number (sole proprietor)
2712	19. Credit/debit card number
2713	20. Business credit card number (sole proprietor)
2714	21. Vehicle Identification Number
2715	22. Business Vehicle Identification Number (sole proprietor)
2716	23. Personal bank account number
2717	24. Business bank account number (sole proprietor)
2718	25. Personal device identifiers or serial numbers
2719	26. Business device identifiers or serial numbers (sole proprietor)
2720	27. Personal mobile number
2721	28. Business mobile number (sole proprietor)
2722	29. Other (please identify)
2723	B. Biographical Information (DESIGN NOTE: Multi select and for sub questions "a., b., c."
2724	repeated for each response selected.)
2725	1. Full name (First, Last, including nicknames)
2726	a. Provide count
2727	b. Is this count known or approximate? (Known/Approximate)
2728	c. Did potential or confirmed access occur? (Potential/Confirmed)
2729	2. Gender
2730	3. Race
2731	4. Date of birth (day, month, year)

2732	5. Ethnicity
2733	6. Nationality
2734	7. Country of birth
2735	8. City or county of birth
2736	9. State of birth
2737	10. Marital status
2738	11. Citizenship
2739	12. Immigration status
2740	13. Religion/religious preference
2741	14. Home address
2742	15. Zip code
2743	16. Home phone or fax number
2744	17. Spouse information
2745	18. Sexual orientation
2746	19. Children information
2747	20. Group/organization membership
2748	21. Military service information
2749	22. Mother's maiden name
2750	23. Business mailing address (sole proprietor)
2751	24. Business phone or fax number (sole proprietor)
2752	25. Global positioning system (GPS)/location data
2753	26. Personal email address
2754	27. Business email address
2755	28. Employment information
2756	29. Personal financial information (including loan information, but not including
2757	account or payment card numbers)
2758	30. Business financial information (including loan information, but not including
2759	account or payment card numbers)
2760	31. Alias (i.e., username or screenname)
2761	32. Education information
2762	33. Resume or curriculum vitae (DISPLAY NOTE: If these documents include additional
2763	types of PII, e.g., address or SSN, please indicate those fields separately.)
2764	34. Professional/personal references (DISPLAY NOTE: If these documents include
2765	additional types of PII, e.g., address or SSN, please indicate those fields separately.)
2766	C. Biometrics, Distinguishing Features, and Characteristics (Design Note"
2767	Multi select and for sub questions "a., b., c.", repeated for each response selected.)
2768	1. Fingerprints
2769	a. Provide count
2770	b. Is this count known or approximate? (Known/Approximate)
2771	c. Did potential or confirmed access occur? (Potential/Confirmed)
2772	2. Palm prints

2773	3. Vascular scans
2774	4. Retina/iris scans
2775	5. Dental profile
2776	6. Scars, marks, tattoos
2777	7. Hair color
2778	8. Eye color
2779	9. Height
2780	10. Video recording
2781	11. Photos
2782	12. Voice/audio recording
2783	13. DNA sample or profile
2784	14. Signatures
2785	15. Weight
2786	D. Medical/Health and Emergency Information (DESIGN NOTE: Multi select and
2787	for sub questions "a., b., c.", repeated for each response selected.)
2788	1. Physical medical/health information
2789	a. Provide count
2790	b. Is this count known or approximate? (Known/Approximate)
2791	c. Did potential or confirmed access occur? (Potential/Confirmed)
2792	2. Mental health information
2793	3. Disability information
2794	4. Workers' compensation information
2795	5. Patient ID number
2796	6. Emergency contact information
2797	E. Device Information (DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated
2798	for each response selected.)
2799	1. Device settings or preferences (e.g., security level, sharing options,
2800	ringtones)
2801	a. Provide count
2802	b. Is this count known or approximate? (Known/Approximate)
2803	c. Did potential or confirmed access occur? (Potential/Confirmed)
2804	2. Cell tower records (i.e., logs, user location, time, etc.)
2805	3. Network communications data
2806	F. Other Specific Information or File Types (DESIGN NOTE: Multi select and for sub
2807	questions "a., b., c.", repeated for each response selected.)
2808	1. Taxpayer information/Tax return information
2809	a. Provide count
2810	b. Is this count known or approximate? (Known/Approximate)
2811	c. Did potential or confirmed access occur? (Potential/Confirmed)
2812	2. Law enforcement information
2813	3. Security clearance/background check information

2814	4. Civil/criminal history information/police record
2815	5. Academic and professional background information
2816	6. Health information
2817	7. Case files
2818	8. Personnel files
2819	9. Credit history information
2820	10. Other
2821	a. Please provide the other specific information or file type(s)
2822	Incident Stage (A): Security Control(s) [Contributing to
2823	Incident]
2824	78. [Op] + [RR but NOT FISMA or FedRAMP reporting] Please review the "Protect"
2825	section of the CISA Cross-Sector Cybersecurity Performance Goals (CPGs). 61 To
2826	the best of your knowledge, did the implementation (or lack thereof),
2827	misconfiguration, or failure of a security control (as described in CISA's Protect
2828	CPGs). <sup>62</sup> lead to, contribute to, or otherwise factor into your incident? (Yes/No)
2829	A. Yes
2830	i. (DESIGN NOTE: If Yes) Select all that apply [] non-implementation []
2831	misconfiguration and/or [] failure of the security control
2832	B. No
2833	C. Unknown (DESIGN NOTE: If the person selects "Unknown", then DISPLAY NOTE: When and if
2834	during your investigation, you discover knowledge about security controls contributing to the
2835	incident, please return to this question and share any details you can about security controls where
2836	the implementation (or lack thereof), improper configuration, or other aspect of the control led to,
2837	contributed to, or otherwise factored into the incident.)  70 (Conditional if O 70 = Vog) [On] + [DC] Select the applicable control(s) from the
2838	79. {Conditional if Q 79 = Yes} [Op] + [RC] Select the applicable control(s) from the CISA Cybersecurity Performance Goals, "Protect" section. <sup>63</sup> .
2839	
2840 2841	A. Select from [DESIGN NOTE: See Appendix 2 for answer options, multi choice select) (DESIGN NOTE: Repeat for each CPG Protect Control selected)
2842	1. (DISPLAY NOTE: Select one) Was the [] failure, [] misconfiguration, or [] non-
2843	implementation of the control due to a published CVE. <sup>64</sup> (s)?
2844	a. Yes (DESIGN Note: The following "CVE" questions are conditional only if the
2845	reporter selected "YES" to security controls factoring into the incident)
2846	1. What is the CVE(s)?
2847	(DESIGN NOTE: Multi select for Failed, Misconfigured, and Not
2848	implemented) (repeat for each CVE identified)

<sup>61</sup> 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. https://cve.mitre.org/

2849	b. No
2850	c. Unknown
2851	2. Do one or more of the observed TTPs reported earlier in this report relate to
2852	this selected security control? (Yes/No)
2853	a. (DESIGN NOTE: If Yes) Please select from your reported observed
2854	TTPs those that are attributed to this security control (DESIGN NOTE:
2855	Display all TTPs [MITRE ATT&CK and general] that have been reported and
2856	allow user to select one or more TTPs and associate with this/these security
2857	control(s).)
2858	B. Please provide any additional information regarding how security control
2859	implementation, failure, misconfiguration, or non-implementation played a role in
2860	this incident (DESIGN NOTE: Open text) (DISPLAY NOTE: This includes not only any additional
2861	information regarding how failure, misconfiguration, or non-implementation of a control may have
2862	contributed to an incident, but also information regarding any controls that were also effective in
2863 2864	mitigating or detecting the incident, and/or controls that worked and forced the threat actor to pivot to something more complex, etc.)
2865	something more complex, etc.)
2866	80. [FISMA or FedRAMP reporting only] (DISPLAY NOTE: CISA understands the NIST SP
2867	800-53 and NIST SP 800-171 are primary sources to follow when establishing and setting various system
2868	controls under FISMA and FedRAMP requirements. CISA also acknowledges others outside FISMA and
2869	FedRAMP may not be as familiar with these publications. Therefore, CISA has implemented two paths for
2870	identifying security controls that have contributed to the incident. For FISMA and/or FedRAMP reporting
2871	the NIST publications are available to reference. For all other reporting, the "Protect" section of the CISA
2872	Cross-Sector Cybersecurity Performance Goals (CPGs). 65 will be referenced.) To the best of your
2873	knowledge, did the implementation (or lack thereof), misconfiguration, or failure of a
2874	security control (as described in NIST SP 800-53) lead to, contribute to, or otherwise
2875	factor into your incident? (Yes/No)
2876	A. Yes
2877	i. (DESIGN NOTE: If Yes) Select all that apply [] non-implementation []
2878	misconfiguration and/or [] failure of the security control
2879	B. No
2880	C. Unknown (DESIGN NOTE: If the person selects "Unknown", then DISPLAY NOTE: When and if,
2881	during your investigation you discover knowledge about security controls contributing to the incident,
2882	please return to this question and share any details you can about security controls where the
2883	implementation (or lack thereof), improper configuration, or other aspect of the control led to,
2884	contributed to, or otherwise factored into the incident.)
2885	81. {Conditional if Q 81 = Yes} [FISMA and FedRAMP only] (DISPLAY NOTE: To
2886 2887	enhance trends and analysis of security controls between incidents, establishing a common reference is a sound approach. Therefore, CISA has associated the CISA CPGs with a subset of NIST SP 800-53 controls
2888	(NIST SP 800-171 is in development). You will have an opportunity to select this subset first if applicable,
2889	then can select from the remaining NIST SP 800-53 set of controls if necessary.) Select the applicable
2890	control(s) from NIST SP 800-53 (CPG preferred list first), then if applicable select
2891	from the remaining controls.
-051	nom the remaining controls.

 $<sup>^{65} \</sup>underline{\text{Cross-Sector Cybersecurity Performance Goals} \mid \text{CISA}} \text{ ($\underline{\text{https://www.cisa.gov/cross-sector-cybersecurity-performance-goals}$)}$ 

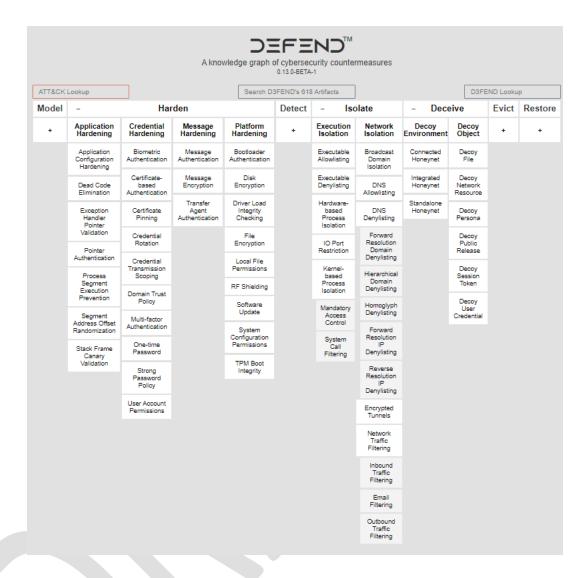
2892	
2893	A. Select from (DESIGN NOTE: provide NIST SP 800-53 subset list per Appendix 2 CPG to NIST SP
2894	800-53 mapping as first dropdown list, then provide another dropdown list identifying remaining
2895	NIST SP 800-53 controls) (DESIGN NOTE: Repeat for each control selected, multi choice select)
2896	1. (DISPLAY NOTE: Select one) Was the [] failure, [] misconfiguration, or [] non-
2897	implementation of the control due to a published CVE. <sup>66</sup> (s)?
2898	a. Yes (DESIGN Note: The following "CVE" questions are conditional only if the
2899	reporter selected "YES" to security controls factoring into the incident)
2900	1. What was the CVE(s)?
2901	(DESIGN NOTE: Multi select for Failed, Misconfigured, and Not
2902	implemented) (repeat for each CVE identified)
2903	b. No
2904	c. Unknown
2905	2. Does one or more of the observed TTPs reported earlier in this report relate
2906	to this selected security control? (Yes/No)
2907	a. (DESIGN NOTE: If Yes) Please select from your reported observed
2908	TTPs the one(s) that are attributed to this security control (DESIGN
2909	NOTE: Display all TTPs [MITRE ATT&CK and general] that have been reported
2910	and allow user to select one or more TTPs and associate with this/these security
2911	control(s).)
2912	B. Please provide any additional information regarding how security control
2913	implementation, failure, misconfiguration, or non-implementation played a role in
2914	this incident (DESIGN NOTE: Open text) (DISPLAY NOTE: This includes not only any additional
2915	information regarding how failure, misconfiguration, or non-implementation of a control may have
2916	contributed to an incident, but also information regarding any controls that were also effective in
2917 2918	mitigating or detecting the incident, and/or controls that worked and forced the threat actor to pivot to something more complex, etc.)
2919	something more complex, etc.)
2313	
2920	o. Containment (C) Stage <sup>67</sup>
2921	82. [Op] + [FISMA Req] Have you begun the containment stage? (Yes/No/Unsure)
2922	(Note: This stage involves taking steps to prevent the incident from spreading
2923	further.)
2924	A. (DESIGN NOTE: If Yes) Provide the date and time (yyyy-mm-dd HH:MM - <utc< td=""></utc<>
2925	offset>) containment activities began
2926	B. Provide an overview of your containment strategy

https://cve.mitre.org/

 $<sup>^{66}</sup>$  Common Vulnerabilities and Exposures (CVE) is a program that identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities.

<sup>&</sup>lt;sup>67</sup> 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]

2927	1. If implementation of the containment strategy is complete, was the
2928	containment strategy successful? (Y/N)
2929	a. (DESIGN NOTE: If No) Provide details on how your strategy is
2930	changing (DESIGN NOTE: Open text)
2931	83. [CUI] {Conditional} [Op] + FISMA Req] What specific containment action(s) have
2932	been taken? (DESIGN NOTE: Can be more than one, include options to add)
2933	A. Description (DESIGN NOTE: Open text)
2934	B. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
2935	C. Has this action been completed? (Yes/No)
2936	1. (DESIGN NOTE: If Yes) Was this action successful? (Yes/No)
2937	a. (DESIGN NOTE: If No) Can you identify why it wasn't successful?
2938	(DESIGN NOTE: Open text)
2939	b. [CUI] (DESIGN NOTE: If No) Provide details on how your
2940	containment action is changing (DESIGN NOTE: Open text)
2941	84. [RC] Have you completed containment? (Yes/No)
2942	
2943	Incident Stage (C): Countermeasures – Containment
2944	85. [Op] + [FISMA Req] As explained earlier, the MITRE D3FEND matrix categorizes
2945	countermeasures into multiple categories. Containment actions are identified in the
2946	"harden," "isolate," and "deceive" categories. Please select the containment actions
2947	you have taken from among these categories. (Select all that apply)
2948	A. Select applicable "containment" counter measures from the MITRE D3FEND list



2949 2950

29502951

29532954

2952

2955

2956 2957

2958

2959 2960

2961

2962

2963

2964

2965

B. [Op] We are unable to use MITRE D3FEND to identify "containment" countermeasures used during this incident, or our organization leveraged a "containment" countermeasure not listed or that is currently unidentified in MITRE D3FEND

1. Did you employ a containment technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No) (DISPLAY NOTE: The top-line categories associated with containment are "harden", "isolate", or "deceive". These are considered the "tactics".)

### (DESIGN NOTE: If Yes)

- a. Which tactic did your containment action fall under?
  - 1. Harden
    - i. Which base technique did your action fall under?
      - 1. Application hardening
      - 2. Credential hardening
      - 3. Message hardening

2966	4. Platform hardening
2967	2. Isolate
2968	i. Which base technique did your action fall under?
2969	1. Execution isolation
2970	2. Network isolation
2971	3. Deceive
2972	i. Which base technique did your action fall under?
2973	1. Decoy environment
2974	2. Decoy object
2975	b. Description (DESIGN NOTE: Open text)
2976	2. (DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify
2977	"containment" countermeasures used during this incident and cannot bucket
2978	the countermeasure into an existing MITRE D3FEND category, please
2979	provide a description and details of the countermeasures you have employed
2980	(DESIGN NOTE: Open text)
2981	C. Unknown
2982	D. None
2983	86. [Op] Please provide any additional context for the "containment" countermeasures
2984	you have taken (DESIGN NOTE: Open text)
2985	p. Eradication Stage <sup>68</sup> (E)
2986	87. [CUI] [Op] + [FISMA Req] Have you begun the eradication stage? (Yes/No/Unsure)
2987	A. [If Yes] Provide the date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
2988	eradication activities began.
2989	1. [CUI] {Conditional} [Op] + [FISMA Req] Provide an overview of your
2990	eradication strategy (DESIGN NOTE: Open text)
2991	2. {Conditional} [Op] + [FISMA Req] Have you completed the eradication
2992	activities? (Yes/No)
2993	a. (DESIGN NOTE: If Yes) Please provide date and time (yyyy-mm-dd
2994	HH:MM - <utc offset="">)</utc>
2995	b. (DESIGN NOTE: If No) Is the implementation of your eradication
2996	strategy complete? (Y/N)
2997	c. (DESIGN NOTE: If No) Was the eradication strategy successful? (Y/N)

<sup>68</sup> 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]

2998			1.	(DES	IGN NO	TE: If No	) Provi	de deta	ails on h	ow you	r eradica	tion
2999		strategy is changing (DESIGN NOTE: Open text)										
3000		d. (DESIGN NOTE: If No) What specific eradication action(s) have been										
3001			tak	en? (D	ESIGN	NOTE: C	an be me	ore than	1, include	options t	o add)	
3002			1.	Desc	cription	n (DESIG	N NOTI	E: Open	text)			
3003			2.	Date	and ti	те (ууу	y-mm	-dd HF	H:MM -	<utc o<="" td=""><td>offset&gt;)</td><td></td></utc>	offset>)	
3004			3.	Has	this ac	tion bee	n com	pleted?	(Yes/N	lo)		
3005				i.	(DESIG	N NOTE:	If Yes)	Was th	is actio	n succe	ssful? (Y	es/No)
3006				ii.	(DESIG	N NOTE:	If No)	Can yo	u identi:	fy why	it wasn't	
3007					succes	sful?						
3008				iii.	(DESIG	N NOTE:	If No)	Provide	e details	on how	your	
3009					eradic	ation ac	tion is	changi	ng.			
3010												
3011	Inciden	t Stage	e (E):	Cou	nter	measi	ıres	– Era	adica	tion		
3012	88. [Op	] + [FISN	//A Req]	As no	ted ear	lier, the	MITR	E D3F	END m	atrix ca	tegorizes	3
3013	cour	ntermeas	ures into	multip	ole cate	egories.	Eradic	ation a	ctions a	re ident	ified in	
3014	МІТ	RE's D3	FEND n	natrix	in the '	'evict" d	ategor	y. Plea	se selec	t the ev	iction ac	tions
3015			en from t									
3016	A. :	Select ap	plicable '	'evict'	' count	ter meas	ures fr	om the	MITRI	E D3FE	ND list:	
3017												
				_		TM						
			A kno	wledge gra	) = F :	END security counte	rmascurac					
			71110	mougo gra	0.13.0-BE							
		ATT&CK Looku	·		ch D3FEND's	818 Artifacts		3FEND Looku				
		Model Ha	rden Detect	Isolate	Deceive	Credential	Evict	Process	Restore			
		+	+ +	•	+	Eviction	Eviction	Eviction	•			
						Account Locking	File Removal	Process Suspension				
						Authentication Cache Invalidation	Email Removal	Process Termination				
						Credential Revoking						
3018												
2010	D	Onl Wa	oro unob	10 to 11	as MIT	TDE D2	CENID	to idea	stifty area	diantia	aguntar	

3019

3020

3021 3022

- B. [Op] We are unable to use MITRE D3FEND to identify eradication counter measures used during this incident, or our organization leveraged an eradication counter measure not listed or that is currently unidentified in MITRE D3FEND.
  - 1. Did you employ a eradication technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No) (DISPLAY NOTE: The top-line category associated with eradication is: "evict". This is considered the "tactics")

(DESIGN NOTE: If Yes) Which evict technique did you action fall under?

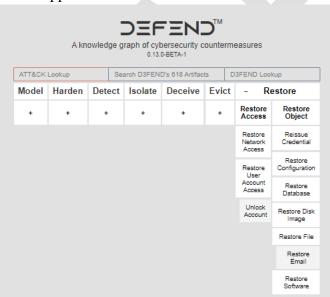
- 1. Credential eviction
  - i. Description

3028	2. File eviction
3029	i. Description
3030	3. Process eviction
3031	i. Description
3032	2. Please provide a description and details of the counter measures you have
3033	employed (DESIGN NOTE: Open text)
3034	C. (DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify "eradication"
3035	counter measures used during this incident and cannot bucket the counter measure
3036	into an existing MITRE D3FEND category, please provide a description and
3037	details of the counter measures you have employed (DESIGN NOTE: Open text)
3038	D. Unknown
3039	E. None
3040	89. [CUI] {Conditional} [Op] + [FISMA Req] Please provide any additional context for
3041	the "eradication" actions you have taken (DESIGN NOTE: Open text)
3042	q. Recovery (R) Stage 69
3043	90. [CUI] [Op] + [FISMA Req] Have you begun the recovery stage? (Yes/No/Unsure)
3044	(DISPLAY NOTE: In the recovery stage, the focus is on restoring affected systems and services to normal
3045	operation.)
3046	A. [RC] (DESIGN NOTE: If Yes)
3047	1. Provide the date and time (yyyy-mm-dd HH:MM - <utc>) Please enter the</utc>
3048	organization's estimated recovery date and time
3049	a. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>
3050	2. [Op] + FISMA Req] Describe your recovery strategy (DESIGN NOTE: open text)
3051	3. [Op] + [FISMA Req] Have you completed the recovery stage and "accepted"
3052	normal operations resumed? (Yes, No)?
3053	a. (DESIGN NOTE: If Yes) Please provide the Date and Time (yyyy-mm-
3054	dd HH:MM - <utc offset="">)</utc>
3055	
3056	4. Was the recovery strategy successful? (Yes/No)
3057	(DESIGN NOTE: If No)
3058	a. Did you modify your strategy after you began recovery? (Yes/No)
3059 3060	[CUI] (DESIGN NOTE: If Yes) Why did you modify the strategy? (DESIGN NOTE: Open text)
3060	(DESIGN NOTE: Open text)
JUUI	

<sup>&</sup>lt;sup>69</sup> 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]

unpredictable; additional

3062	91. [Op] + [RR] Estimate the scope of resources needed to recover from the incident
3063	(recoverability).
3064	A. Regular (DISPLAY NOTE: (Provide hover-over) Time to recover is predictable with existing
3065	resources.)
3066	B. Supplemented (DISPLAY NOTE: (Provide hover-over) Time to recover is predictable with
3067	additional resources.)
3068	C. Extended (DISPLAY NOTE: (Provide hover-over) Time to recover is unpredictable; additional
3069	resources and outside help are needed.)
3070	D. Not recoverable (DISPLAY NOTE: (Provide hover-over) Recovery from the incident is not
3071	possible (i.e., sensitive data exfiltrated and posted publicly).)
3072	
3073	Incident Stage (R): Recovery Actions
3074	92. [Op] + [FISMA Req] As noted earlier, the MITRE D3FEND matrix categorizes
3075	countermeasures into multiple categories. Recovery activities are identified in
3076	MITRE's D3FEND matrix in the "restore" category. Please select the recovery
3077	actions you have taken from this category. Select all that apply.
3078	A. Select applicable "restore" measures from the MITRE D3FEND list:
	A knowledge graph of cybersecurity countermeasures



3079 3080

B. [Op] We are unable to use MITRE D3FEND to identify "recovery" countermeasures used during this incident, or our organization leveraged a "recovery" counter measure not listed or that is currently unidentified in MITRE D3FEND.

3082 3083 3084

3081

1. Did you employ a recovery technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No) (DISPLAY NOTE: The top-line category associated with "recovery" is: "restore." This is considered the "tactic"),

3085 3086 3087

(DESIGN NOTE: If Yes) Which restore technique did your action(s) fall under:

3088

1. Restore access

3089

Description

3090	2. Restore object
3091	i. Description
3092	2. (DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify
3093	"recovery" countermeasures used during this incident, and you cannot bucket
3094	your counter measure into an existing MITRE D3FEND category, please
3095	provide a description and details of the counter measures you have employed.
3096	(DESIGN NOTE: Open text)
3097	C. Unknown
3098	D. None
3099	93. [Op] + [FISMA Req] Please describe any additional recovery steps you have taken
3100	(e.g., additional external outreach and/or support, update any relevant policies,
3101	procedures, and plans, such as incident response plans, continuity of business plans,
3102	disaster recovery plans, system back-up and restore plans, business exercise plans)
3103	(DESIGN NOTE: Open text)
3104	
3105	r. Post-Incident (P-I) Stage
3106	94. [Op] + [FISMA Req] Has the incident concluded? (Yes/No)
3107	(DESIGN NOTE: If Yes) Provide your post incident report/details
2100	A [On] + [FISMA Peal If evailable submit any next incident or often action reports
3108	A. [Op] + [FISMA Req] If available, submit any post incident or after-action reports related to this incident (Submit your organization's post incident report (WITH AN UPLOAD FILE
3109 3110	OPTION HERE.) (DISPLAY NOTE: For Federal civilian executive branch agencies, this is in line with
3111	CISA's Incident Playbook to allow CISA to "validate organization's response".). 70
3112	B. [Op] + [FISMA Req] Looking back on your incident response, was there
3113	information that, had you received it or learned it sooner, would have led to a
3114	more streamlined, quicker, and/or more effective incident response? If yes,
3115	identify the incident response stage where you would have preferred to receive
3116	this information. (DESIGN NOTE: Multi select; based on NIST 800-61 r2, the major phases of an
3117	incident life cycle.)
3118	1. Identification and detection
3119	a. Which organization could have provided the information? (DESIGN
3120	NOTE: Repeated for each stage selected.)
3121	2. Analysis
3122	3. Containment
3123	4. Eradication
3124	5. Recovery
3125	6. Post-incident

<sup>&</sup>lt;sup>70</sup> Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems: Publication: November 2021

3126	C. [Op] + [FISMA Req] Has the impacted organization performed a review of the
3127	incident and incident response to identify lessons learned? (Y/N)
3128	1. (DESIGN NOTE: If Yes) Please describe the identified lessons learned in the areas
3129	of:
3130	a. Incident handling processes
3131	b. Mean time to effective analysis
3132	c. Mean time to detection
3133	d. Mean time to response
3134	e. Mean time to defense
3135	f. Mean time to reporting
3136	g. Other
3137	D. [Op] + [FISMA Req] Based on your experience in this incident, please provide
3138	recommendations on how CISA can improve the support it provides
3139	1. What could CISA do differently in future incidents? (DESIGN NOTE: Open text)
3140	2. Are there indicators of compromise or relevant detection mechanisms you
3141	have not provided previously in this report and believe can enable detection
3142	of similar incidents in the future? (DESIGN NOTE: Open text)
3143	3. What additional tools or resources would you need to detect, analyze, and
3144	mitigate future incidents? (DESIGN NOTE: Open text)
3145	

3146	s. Event Reporting (Below Incident Thresholds)							
3147	(FISMA – Only)							
3148	(DESIGN NOTE: FISMA Only – If reporter answers "NO" to all CIA Impact Assessments)							
	Confidentiality, Integrity, Availability Assessment <sup>20</sup>							
	21. [RA] (DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event-							
	Incident FLAG for FISMA reporters only. If Q21 A-C are answered "no", that terminates the rest 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 actually							
	jeopardize, without lawful authority, any of the following relating to either 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							
	"actually" selected, the other two options can be "unsure" or "none" if applicable, otherwise if all are "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 NOTE: 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 <sup>22</sup> [] imminently; [] actually; [] unsure []/none (DESIGN NOTE: Have							
	radio button for all)							
	B. integrity, <sup>23</sup> [] imminently; [] actually; [] unsure/none (DESIGN NOTE: Have radio button for all)							
2140	C. availability <sup>24</sup> [] imminently; [] actually; [] unsure/none (DESIGN NOTE: Have radio button for all)							
3149 3150	95. [FISMA Req] Has this activity already been reported? (Yes/No)							
3151	A. (DESIGN NOTE: If Yes) Provide							
3152	1. Incident report form submission number.							
3153	2. CISA incident tracking number.							
3154	96. [CUI] [FISMA Req] Describe the scope of impacted systems and provide a high-level							
3155	summary of the event activity. (DESIGN NOTE: Narrative of the event detection)							
3156	97. [FISMA Req] When did you first detect the activity?							
3157	A. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>							
3158	98. [FISMA Req] When did you declare an event?							
3159	A. Date and time (yyyy-mm-dd HH:MM - <utc offset="">)</utc>							
3160	99. [FISMA Req] Please provide any additional information relevant to the event (DESIGN							
3161	NOTE: Open text)							
3162	100. [FISMA Req] Has the entity covered by this event resolved the consequences for							
3163	the event? (Yes/No)							
3164	A. (DESIGN NOTE: If Yes) Provide the date and time when the event was resolved							
3165	<ol> <li>Recovered as of date/time (yyyy-mm-dd HH:MM -<utc offset="">)</utc></li> </ol>							
3166	101. [FISMA Req] Please describe any additional steps you have taken to resolve the							
3167	event (e.g., additional external outreach and/or support, update any relevant policies,							
3168	procedures, and plans, such as incident response plans, continuity of business plans,							
3169	disaster recovery plans, system back-up and restore plans, business exercise plans)							
3170	(DESIGN NOTE: Open text)							

3171	t. Data Marking Stage
3172	Cybersecurity Information Sharing Act of 2015
3173	Acknowledgement
3174	(DESIGN NOTE: Only Show for Non-Federal Voluntary Reporters [i.e., Voluntary Report] or Non-
3175	Federal Non-Voluntary Reporters [e.g., TSA], not to be shown for FISMA reporters)
3176	102. [Op] + [Not Applicable to FISMA Reporting] To the extent not already indicated
3177	using the data markings, do your responses to any of the questions above constitute
3178	cyber threat indicator(s) or defensive measure(s) submitted under the Cybersecurity
3179	Information Sharing Act of 2015 that the submitter is requesting be treated as
3180	commercial, financial, and proprietary? (Yes/No)
3181	A. (DESIGN NOTE: If Yes) Select question numbers (DESIGN NOTE: Provide drop-down, multi
3182	select).
3183	
3184	Overall Report Data Markings
3185	103. [CUI] [Op] + [RR] The most restrictive marking that has been reported in this
3186	incident is X <sup>71</sup> Is this a valid marking for the entire incident? (Yes/No)
3187	A. (DESIGN NOTE: If Yes) Then the incident marking is X. <sup>72</sup>
3188	B. (DESIGN NOTE: If No) User to enter new marking for the entire incident
3189	(DESIGN NOTE: See Appendix 1 for question options. 73)
3190	
2404	u.End of Incident Reporting Questions
3191	u. End of incluent Reporting Questions
3192	
3193	v. Appendix 1: Data Marking
2404	Data Marking Options
3194	Data Warking Options
3195	
3196	1. Specific data marking options are as follows
3197	1. [C-15] Cybersecurity Information Sharing Act of 2015 commercial, financial, and
3198	proprietary. <sup>74</sup>
3199	2. [CUI] Controlled unclassified information (CUI). <sup>75</sup>

The default data marking presented here.
 The accepted default data marking here.
 Option to change default data marking.

<sup>&</sup>lt;sup>74</sup> 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

# Protect CISA CPGs & NIST SP 800-53 References

3200

3201

3202

3203 3204

CPG #	Additional Reference(s) [including NIST 800-53 for FISMA reports]	Security Practice	Outcome	TTP or Risk Addressed	Recommended Action
2.A	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	Changing default passwords	Prevent threat actors from using default passwords to achieve initial access or move laterally in a network.	Valid accounts - default accounts (T1078.001) Valid accounts (ICS T0859)	An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for operational technology, such as operational technology administration web pages.  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.  Operational technology: While changing default passwords on an 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.

 $<sup>{}^{76}\,\</sup>underline{Cross-Sector}\,\underline{Cybersecurity}\,\underline{Performance}\,\,\underline{Goals}\,\,|\,\,\underline{CISA}\,\,(\underline{https://www.cisa.gov/cross-sector-cybersecurity-performance-goals})$ 

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 systemenforced 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 bruteforce 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, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 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, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 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 Interface (HMIs.)
2.I	NIST SP 800- 53: AT-2 ISA 62443-2- 1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1	Basic cybersecurity training	Organizational users learn and perform more secure behaviors	User training (M1017, ICS M0917)	At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness.  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 ISA 62443-2- 1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2	Operational technology cybersecurity training	Personnel responsible for securing operational technology assets received specialized operational technology- focused cybersecurity training	User training (M1017, ICS M0917)	In addition to basic cybersecurity training, personnel who maintain or secure operational technology as part of their regular duties receive operational technology-specific cybersecurity training on at least an annual basis.

	_				
2.K	NIST SP 800-	Strong and agile	Effective	Adversary-in-the-	Properly configured and up-to-date
	53: SC-8, SC-	encryption	encryption	middle (T1557)	secure socket layer (SSL) / transport
	13, SC-28		deployed to	Automated collection	layer security (TLS) is utilized to
	ISA 62443-3-		maintain	(T1119)	protect data in transit, when
	3:2013 SR 3.1,		confidentiality of	Network sniffing	technically feasible. Organizations
	SR 3.4, SR 3.8,		sensitive data and	(T1040, ICS T0842)	should also plan to identify any use
	SR 4.1, SR 4.2		integrity of IT	Wireless compromise	of outdated or weak encryption,
	ISO/IEC		and operational	(ICS T0860)	update these to sufficiently strong
	27001:2013			Wireless sniffing (ICS	algorithms, and consider managing
			technology traffic		
	A.8.2.3,			T0887)	the implications of post-quantum
	A.13.1.1,				cryptography.
	A.13.2.1,				
	A.13.2.3,				Operational technology: To minimize
	A.14.1.2,				the impact to latency and availability,
	A.14.1.3				encryption is used when feasible,
					usually for operational technology
					communications connecting with
					remote/external assets.
2.L	NIST SP 800-	Secure sensitive	Protect sensitive	Unsecured credentials	Sensitive data, including credentials,
	53 Rev. 4 AC-	data	information from	(T1552)	are not stored in plaintext anywhere
	4, AC-5, AC-6,		unauthorized	Steal or forge	in the organization and can only be
	MP-12, PE-19,		access	Kerberos tickets	accessed by authenticated and
	PS-3, PS-6, SC-			(T1558)	authorized users. Credentials are
	7, SC-8, SC-11,			OS credential	stored in a secure manner, such as
	SC-12, SC-13,			dumping (T1003)	with a credential/password manager
	SC-28, SC-31,			Data from information	or vault, or other privileged account
	SI-4			repositories (ICS	management solution.
	ISA 62443-3-			T0811)	management solution.
				Theft of operational	
	3:2013 SR 3.4,				
	SR 4.1, SR 5.2			information (T0882)	
	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.9.1.2,			ľ	
	A.9.2.3,				
	A.9.4.1,				
	A.9.4.4,				
	A.9.4.5,				
	A.10.1.1,				
	A.11.1.4,				
	A.11.1.5,				
	A.11.2.1,				
	A.13.1.1,				
	A.13.1.3,				
	A.13.2.1,				
	A.13.2.3,				
	A.13.2.4,				
	A.14.1.2,				
	A.14.1.3				
L	11.17.1.√	1	<u>l</u>	l	

	T				
2.M	NIST SP 800-	Email security	Reduce risk from	Phishing (T1566)	On all corporate email infrastructure
	53 Rev. 4 AC-		common email-	business email	(1) STARTTLS is enabled, (2)
	4, AC-5, AC-6,		based threats,	compromise	Sender Policy Framework (SPF) and
	CM-8, MP-6,		such as spoofing,		DomainKeys Identified Mail (DKIM)
	MP-8, PE-16,		phishing, and		are enabled, and (3) Domain-based
	PE-19, PS-3,		interception		Message Authentication, Reporting,
	PS-6, SC-7,				and Conformance (DMARC) is
	SC-8, SC-11,				enabled and set to "reject." For
	SC-12, SC-13,				further examples and information, see
	SC-28, SC-31,				CISA's past guidance for federal
	SI-4				agencies at <link bod="" to=""/> :
	ISA 62443-3-				https://www.cisa.gov/binding-
	3:2013 SR 3.1,				operational-directive-18-01
	SR 3.4, SR. 3.8,				
	SR 4.1, SR 4.1,				
	SR 4.2, SR 5.2				
2.N	NIST SP 800-	Disable macros	Reduce the risk	Phishing -	A system-enforced policy that
	53: CM-10,	by default	from embedded	spearphishing	disables Microsoft Office macros, or
	CM-11, SC-13		macros and	attachment	similar embedded code, by default on
	ISA 62443-2-		similar executive	(T1566.001)	all devices. If macros must be
	1:2009		code, a common	User execution -	enabled in specific circumstances,
	4.3.4.3.2,		and highly	malicious File	there is a policy for authorized users
	4.3.4.3.3		effective threat	(T1204.002)	to request that macros are enabled on
	ISA 62443-3-		actor TTP		specific assets.
	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,				
2.0	A.14.2.4 NIST SP 800-	D	M	Dalamad insufficient	Oititi
2.0		Document device	More efficiently	Delayed, insufficient,	Organizations maintain accurate
	53: CM-2, CM-		and effectively	or incomplete ability	documentation describing the
	6, CM-8	configurations	manage, respond	to maintain or restore	baseline and current configuration details of all critical IT and
	ISA 62443-2- 1:2009		to, and recover from cyberattacks	functionality of critical devices and service	
				operations.	operational technology assets to facilitate more effective vulnerability
	4.3.4.3.2,		against the	operations.	
	4.3.4.3.3 ISA 62443-3-		organization and maintain service		management and response and recovery activities. Periodic reviews
	3:2013 SR 7.6		continuity		and updates are performed and
	3:2013 SR 7.6 ISO/IEC		COMMINITALIV		
					tracked on a recurring basis.
	27001:2013				
1	27001:2013 A.12.1.2,				
	27001:2013 A.12.1.2, A.12.5.1,				
	27001:2013 A.12.1.2, A.12.5.1, A.12.6.2,				
	27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2,				
	27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3,				
2 D	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	Dogument		Incomplete or	tracked on a recurring basis.
2.P	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 NIST SP 800-	Document Network	More efficiently	Incomplete or inaccurate	tracked on a recurring basis.  Organizations maintain accurate
2.P	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 NIST SP 800- 53: CM-2, CM-	Network	More efficiently and effectively	inaccurate	Organizations maintain accurate documentation describing updated
2.P	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 NIST SP 800- 53: CM-2, CM- 6, CM-8		More efficiently and effectively respond to	inaccurate understanding of	Organizations maintain accurate documentation describing updated network topology and relevant
2.P	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 NIST SP 800- 53: CM-2, CM- 6, CM-8 ISA 62443-2-	Network	More efficiently and effectively respond to cyberattacks and	inaccurate understanding of network topology	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and
2.P	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 NIST SP 800- 53: CM-2, CM- 6, CM-8 ISA 62443-2- 1:2009	Network	More efficiently and effectively respond to cyberattacks and maintain service	inaccurate understanding of network topology inhibits effective	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and operational technology networks.
2.P	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 NIST SP 800- 53: CM-2, CM- 6, CM-8 ISA 62443-2- 1:2009 4.3.4.3.2,	Network	More efficiently and effectively respond to cyberattacks and	inaccurate understanding of network topology inhibits effective incident response and	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and operational technology networks. Periodic reviews and updates should
2.P	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 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	Network	More efficiently and effectively respond to cyberattacks and maintain service	inaccurate understanding of network topology inhibits effective	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
2.P	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 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-	Network	More efficiently and effectively respond to cyberattacks and maintain service	inaccurate understanding of network topology inhibits effective incident response and	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and operational technology networks. Periodic reviews and updates should
2.P	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 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	Network	More efficiently and effectively respond to cyberattacks and maintain service	inaccurate understanding of network topology inhibits effective incident response and	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
2.P	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 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	Network	More efficiently and effectively respond to cyberattacks and maintain service	inaccurate understanding of network topology inhibits effective incident response and	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
2.P	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 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	Network	More efficiently and effectively respond to cyberattacks and maintain service	inaccurate understanding of network topology inhibits effective incident response and	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

	A.12.5.1, A.12.6.2,				
	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		and reduce the	Hardware additions	firmware, or software/software
	ISA 62443-2-		likelihood of	(T1200)	version is installed or deployed.
	1:2009		breach by users	Browser extensions	Organizations maintain a risk-
	4.3.4.3.2,		installing	(T1176)	informed allowlist of approved
	4.3.4.3.3		unapproved	Transient cyber asset	hardware, firmware, and software
	ISA 62443-3-		hardware,	(ICS T0864)	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,				
2.R	A.14.2.4	C	0	Data destruction	A 11
2.K	NIST SP 800-	System Backups	Organizations reduce the	(T1485, ICS T0809)	All systems that are necessary for operations are regularly backed up on
	53: CP-6, CP-9, CP-10		likelihood and	Data encrypted for	a regular cadence (no less than once
	ISA 62443-2-		duration of data	impact (T1486)	per year).
	1:2009 4.3.4.3.9		loss at loss of	Disk wipe (T1561)	per year).
	ISA 62443-3-		service delivery	Inhibit system	Backups are stored separately from
	3:2013 SR 7.3,		or operations	recovery (T1490)	the source systems and tested on a
	SR 7.4			Denial of control (ICS	recurring basis, no less than once per
	ISO/IEC			T0813)	year. Stored information for
	27001:2013			Denial/loss of view	operational technology assets
	A.12.3.1,			(ICS T0815, T0829)	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,	
2.7	NHOTE OF COO	T '1	0 : ::	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 ISA 62443-2-	Plans	practice, and update	contain, mitigate, and communicate about	technology cybersecurity incident 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
	4.3.4.5.11				are drilled at least annually and are
	ISA 62443-3-				updated within a risk-informed time
	3:2013 SR 3.3				frame following the lessons learned
	ISO/IEC				portion of any exercise or drill.
	27001:2013				
	A.16.1.1,				
	A.17.1.1,				
	A.17.1.2,				
	A.17.1.3				

2.T	NIST SP 800-	Log Collection	Achieve better	Delayed, insufficient,	Access- and security-focused logs
	53: AU-2, AU-		visibility to	or incomplete ability	(e.g., intrusion detection
j	3, AU-7, AU-9,		detect and	to detect and respond	systems/intrusion prevention systems,
	AU-11		effectively	to potential cyber	firewall, data loss prevention, virtual
	ISA 62443-2-		respond to	incidents	private network) are collected and
	1:2009 4.3.3.3.9,		cyberattacks	Impair defenses (T1562)	stored for use in both detection and incident response activities (e.g.,
ĺ				(11302)	
	4.3.3.5.8, 4.3.4.4.7,				forensics). Security teams are notified when a critical log source is disabled,
ĺ	4.4.2.1, 4.4.2.2,				such as Windows event logging.
	4.4.2.1, 4.4.2.2,				such as windows event logging.
1	ISA 62443-3-				Operational technology: For
	3:2013 SR 2.8,				operational technology assets where
	SR 2.9, SR				logs are non-standard or not
	2.10, SR 2.11,				available, network traffic and
l i	SR 2.12				communications between those assets
	ISO/IEC				and other assets is collected.
	27001:2013				
	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-	Secure Log	Organizations'	Indicator removal on	Logs are stored in a central system,
1	53: AU-2, AU-	Storage	security logs are	host - clear Windows	such as a security information and
	3, AU-7, AU-9,		protected from	event logs	event management tool or central
	AU-11		unauthorized	(T1070.001)	database and can only be accessed or
	ISA 62443-2-		access and	Indicator removal on	modified by authorized and
	1:2009		tampering	host - Clear Linux or	authenticated users. Logs are stored
	4.3.3.3.9,			Mac system logs	for a duration informed by risk or
	4.3.3.5.8, 4.3.4.4.7,			(T1070.002) Indicator removal on	pertinent regulatory guidelines.
	4.3.4.4.7, 4.4.2.2,			host - file deletion	
	4.4.2.1, 4.4.2.2,			(T1070.004)	
	ISA 62443-3-			Indicator removal on	
	3:2013 SR 2.8,			host (ICS T0872)	
	SR 2.9, SR			1051 (105 100 /2)	
	2.10, SR 2.11,				
	SR 2.12				
	ISO/IEC			)	
1	27001:2013				
	A.12.4.1,				
1	A.12.4.2,				
	A.12.4.3,				
	A.12.4.4,				
	A.12.7.1				
2.V	NIST SP 800-	Prohibit	Prevent malicious	Hardware additions	Organizations maintain policies and
	53: MP-2, MP-	Connection of	actors from	(T1200)	processes to ensure that unauthorized
] 1	7	Unauthorized	achieving initial	Replication through	media and hardware are not
1	ISA 62443-3-	Devices	access or data exfiltration via	removable media	connected to IT and operational
] 1	3:2013 SR 2.3		unauthorized	(T1091, ICS T0847)	technology assets, such as by limiting use of USB devices and removable
	ISO/IEC 27001:2013				
1	A.8.2.1,		portable media devices		media or disabling AutoRun.
	A.8.2.1, A.8.2.2,		uevices		Operational technology: When
	A.8.2.3,				feasible, establish procedures to
	A.8.3.1,				remove, disable, or otherwise secure
	A.8.3.3,				physical ports to prevent the
	A.11.2.9				connection of unauthorized devices
1					or establish procedures for granting
					access through approved exceptions.
	l	<u>l</u>	<u>l</u>	<u> </u>	acceptions.

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	Č
	ISO/IEC			T0822)	
	27001:2013			Remote services -	
	A.13.1.1,			remote desktop	
	A.13.2.1,			protocol (T1021.001)	
	A.14.1.3				
2.X	NIST SP 800-	Limit	Reduce the risk	Active scanning -	No operational technology assets are
	53: AC-4, SC-	operational	of threat actors	vulnerability scanning	on the public internet, unless
	7, SC-32, SC-	technology	exploiting or	(T1595.002)	explicitly required for operation.
	39	connections to	interrupting OT	Exploit public-facing	Exceptions must be justified and
	ISA 62443-3-	public Internet	assets connected	application (T1190,	documented, and excepted assets
	3:2013 SR 3.1,		to the public	ICS T0819)	must have additional protections in
	SR 3.5, SR 3.8,				
			internet	Exploitation of remote	place to prevent and detect
I	SR 4.1, SR 4.3,		internet	service (T1210, ICS	exploitation attempts (such as
			internet	service (T1210, ICS T0866)	exploitation attempts (such as logging, MFA, mandatory access via
	SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,		internet	service (T1210, ICS T0866) External remote	exploitation attempts (such as
	SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6		internet	service (T1210, ICS T0866) External remote services (T1133, ICS	exploitation attempts (such as logging, MFA, mandatory access via
	SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC		internet	service (T1210, ICS T0866) External remote	exploitation attempts (such as logging, MFA, mandatory access via
	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		internet	service (T1210, ICS T0866) External remote services (T1133, ICS	exploitation attempts (such as logging, MFA, mandatory access via
	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,		internet	service (T1210, ICS T0866) External remote services (T1133, ICS	exploitation attempts (such as logging, MFA, mandatory access via
	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		internet	service (T1210, ICS T0866) External remote services (T1133, ICS	exploitation attempts (such as logging, MFA, mandatory access via

3205

3206

3209

3210

3211

3212

3213

3214

3215

3216

3217

3218

# x. Appendix 3: Incident Type/Categories

Incident Types involving Malware (based on <u>VERIS</u> with some modifications.<sup>77</sup>):

- 3208 1. Adware
  - 2. Backdoor (enable remote access)
  - 3. Brute force attack
  - 4. Capture data from application or system process
  - 5. Capture data stored on system disk
  - 6. Client-side attack (client-side or browser attack (e.g., redirection, XSS, MitB))
  - 7. Click fraud or Bitcoin mining
  - 8. C2 (command and control)
  - 9. Destroy data (destroy or corrupt stored data)
  - 10. Disable controls (disable or interfere with security controls)
- 3219 11. DoS (denial of service attack)
- 3220 12. Downloader (pull updates or other malware)
- 3221 13. Exploit vulnerability in code (vs misconfiguration or weakness)

-

<sup>&</sup>lt;sup>77</sup> Enumerations (verisframework.org)

2222	14. Francis de de la considera
3222	14. Export data to another site or system
3223	15. Packet sniffer (capture data from network)
3224	16. Password dumper (extract credential hashes)
3225	17. RAM scraper or memory parser (capture data from volatile memory)
3226	18. Ransomware (encrypt or seize stored data)
3227	19. Rootkit (maintain local privileges and stealth)
3228	20. Scan network (scan or footprint network)
3229	21. Spam (send spam)
3230	22. Spyware/Keylogger (spyware, keylogger or form-grabber (capture user input
3231	or activity))
3232	23. SQL injection attack
3233	24. Adminware (system or network utilities (e.g., PsTools, Netcat))
3234	25. Worm (propagate to other systems or devices)
3235	
3236	Incident Types Involving Hacking (based on <u>VERIS</u> with some modifications <sup>78</sup> ):
3237	1. Abuse of functionality
3238	2. Brute force or password guessing attacks
3239	3. Buffer overflow
3240	4. Cache poisoning
3241	5. Session prediction: Credential or session prediction
3242	6. CSRF: Cross-site request forgery
3243	7. XSS: Cross-site scripting
3244	8. Cryptanalysis
3245	9. DoS: Denial of service
3246	10. Foot-printing and fingerprinting
3247	11. Forced browsing or predictable resource location
3248	12. Format string attack
3249	13. Fuzz testing
3250	14. HTTP request smuggling
3251	15. HTTP request splitting
3252	16. Integer overflows
3253	17. LDAP injection
3254	18. Mail command injection
3255	19. MitM: Man-in-the-middle attack
3256	20. Null byte injection
3257	21. Offline cracking: Offline password or key cracking (e.g., rainbow tables,
3258	Hashcat, JtR)
3259	22. OS commanding

<sup>78</sup> Enumerations (verisframework.org)

Page 100 of 120

3260	23. Path traversal
3261	24. RFI: Remote file inclusion
3262	25. Reverse engineering
3263	26. Routing detour
3264	27. Session fixation
3265	28. Session replay
3266	29. Soap array abuse
3267	30. Special element injection
3268	31. SQL injection
3269	32. SSI injection
3270	33. URL redirector abuse
3271	34. Use of backdoor or C2
3272	35. Use of stolen creds
3273	36. XML attribute blowup
3274	37. XML entity expansion
3275	38. XML external entities
3276	39. XML injection
3277	40. XPath injection
3278	41. XQuery injection
3279	42. Virtual machine escape
3280	
3281	Incident Types Involving Social Engineering (based on VERIS with some
3282	modifications. <sup>79</sup> ):
3283	1. Baiting (planting infected media)
3284	2. Bribery or solicitation
3285	3. Elicitation (subtle extraction of info through conversation)
3286	4. Extortion or blackmail
3287	5. Forgery or counterfeiting (fake hardware, software, documents, etc.)
3288	6. Influence tactics (leveraging authority or obligation, framing, etc.)
3289	7. Scam (online scam or hoax (e.g., scareware, 419 scam, auction fraud))
3290	8. Phishing (or any type of *ishing)
3291	9. Pretexting (dialogue leveraging invented scenario)
3292	10. Propaganda or disinformation
3293	11. Spam (unsolicited or undesired email and advertisements)
3294	
3295	
3296	Incident Types Involving Misuse of Assets [sometimes called "Insider
3297	Threats"] (based on <u>VERIS</u> with some modifications <sup>80</sup> ):

<sup>79</sup> Enumerations (verisframework.org)
 <sup>80</sup> Enumerations (verisframework.org)

3298	1.	Knowledge abuse: Abuse of private or entrusted knowledge
3299	2.	Privilege abuse: Abuse of system access privileges
3300	3.	Embezzlement, skimming, and related fraud
3301	4.	Data mishandling: Handling of data in an unapproved manner
3302	5.	Email misuse: Inappropriate use of email or IM
3303	6.	Net misuse: Inappropriate use of network or Web access
3304	7.	Illicit content: Storage or distribution of illicit content
3305	8.	Unapproved workaround or shortcut
3306	9.	Unapproved hardware: Use of unapproved hardware or devices
3307	10.	Unapproved software: Use of unapproved software or services
3308		
3309	Incident Typ	es Involving Physical Actions (based on VERIS with some
3310	modifications .81):	
3311	1.	Assault (threats or acts of physical violence)
3312	2.	Sabotage (deliberate damaging or disabling)
3313	3.	Snooping (sneak about to gain info or access)
3314	4.	Surveillance (monitoring and observation)
3315	5.	Tampering (alter physical form or function)
3316	6.	Theft (taking assets without permission)
3317	7.	Wiretapping (Physical tap to comms line)
3318		
3319	Incident Typ	oes Involving Human (or Technology) Errors (based on
3320	<u>VERIS</u> with some m	
3321	1.	`
3322	2.	Data entry error
3323	3.	Disposal error
3324	4.	Gaffe (social or verbal slip)
3325		Loss or misplacement
3326	6.	Maintenance error
3327	7.	Misconfiguration
3328		Misdelivery (direct or deliver to wrong recipient)
3329	9.	Omission (something intended, but not done)
3330		Physical accidents (e.g., drops, bumps, spills)
3331	11.	Capacity shortage (poor capacity planning)
3332	12.	Programming error (flaws or bugs in custom code)
3333	13.	Publishing error (private info to public doc or site)
3334	14.	Malfunction (technical malfunction or glitch)
3335		

81 Enumerations (verisframework.org)
82 Enumerations (verisframework.org)

3336	Incident Types Involving Environmental Factors (based on VERIS with
3337	some modifications. <sup>83</sup> ):
3338	1. Deterioration and degradation
3339	2. Earthquake
3340	3. EMI: Electromagnetic interference (EMI)
3341	4. ESD: Electrostatic discharge (ESD)
3342	5. Temperature: Extreme temperature
3343	6. Fire
3344	7. Flood
3345	8. Hazmat: Hazardous material
3346	9. Humidity
3347	10. Hurricane
3348	11. Ice and snow
3349	12. Landslide
3350	13. Lightning
3351	14. Meteorite
3352	15. Particulates: Particulate matter (e.g., dust, smoke)
3353	16. Pathogen
3354	17. Power failure or fluctuation
3355	18. Tornado
3356	19. Tsunami
3357	20. Vermin
3358	21. Volcanic eruption
3359	22. Leak: Water leak
3360	23. Wind
3361	y. Appendix 4: Critical Infrastructure Sectors and
3362	Subsectors
3363	Format of list is as follows:
3364	• Sector
3365	o Subsector
3366	• Chemical
3367	<ul> <li>Chemical manufacturing or processing plant</li> </ul>
3368	o Chemical transport
3369	Chemical storage warehousing and storage
3370	o Chemical end user
3371	Regulatory, oversight, or industry organization
3372	Commercial facilities

<sup>83</sup> Enumerations (verisframework.org)

3373		<ul> <li>Entertainment and media</li> </ul>
3374		<ul> <li>Gaming</li> </ul>
3375		<ul> <li>Lodging</li> </ul>
3376		<ul> <li>Outdoor events</li> </ul>
3377		<ul> <li>Public assembly</li> </ul>
3378		o Real estate
3379		o Retail
3380		<ul> <li>Sports leagues</li> </ul>
3381	•	Communications
3382		<ul> <li>Information services</li> </ul>
3383		<ul> <li>Telecommunications</li> </ul>
3384		<ul> <li>Regulatory, oversight, or industry organization</li> </ul>
3385	•	Critical Manufacturing
3386		o Primary metal manufacturing
3387		<ul> <li>Machinery manufacturing</li> </ul>
3388		o Electrical equipment, appliance, and component manufacturing
3389		<ul> <li>Transportation manufacturing</li> </ul>
3390		<ul> <li>Non-critical manufacturing facility</li> </ul>
3391	•	Dams
3392		<ul> <li>Dam project</li> </ul>
3393		<ul> <li>Dams control operations facility</li> </ul>
3394		<ul> <li>Levees and hurricane barriers</li> </ul>
3395		<ul> <li>Navigation locks</li> </ul>
3396		<ul> <li>Mine tailing and industrial waste impoundment</li> </ul>
3397		<ul> <li>Regulatory, oversight, or industry organization</li> </ul>
3398	•	Defense industrial base
3399		<ul> <li>Defense manufacturing facility</li> </ul>
3400		<ul> <li>Defense research and development facility</li> </ul>
3401		<ul> <li>Defense logistics and asset management facility</li> </ul>
3402		<ul> <li>Defense industrial base administration and regulatory facility</li> </ul>
3403	•	Emergency services
3404		<ul> <li>Law enforcement</li> </ul>
3405		<ul> <li>Fire and emergency services</li> </ul>
3406		<ul> <li>Emergency medical services</li> </ul>
3407		<ul> <li>Emergency management</li> </ul>
3408		<ul> <li>Public works</li> </ul>
3409		<ul> <li>Emergency communication</li> </ul>
3410	•	Energy
3411		o Electricity
3412		o Petroleum
3413		o Natural gas
3414		o Coal
3415		o Ethanol

3416		o Biodiesel
3417		<ul> <li>Hydrogen</li> </ul>
3418	•	Financial Services
3419		<ul> <li>Banking and credit</li> </ul>
3420		<ul> <li>Securities, commodities, or financial investment</li> </ul>
3421		<ul> <li>Insurance company</li> </ul>
3422	•	Food and agriculture
3423		<ul> <li>Supply</li> </ul>
3424		<ul> <li>Processing, packaging, and production</li> </ul>
3425		<ul> <li>Agriculture and food product storage and distribution warehouse</li> </ul>
3426		<ul> <li>Agriculture and food product transportation</li> </ul>
3427		<ul> <li>Agriculture and food product distribution</li> </ul>
3428		<ul> <li>Agriculture and food supporting facility</li> </ul>
3429		<ul> <li>Regulatory, oversight, or industry organization</li> </ul>
3430	•	Government facilities
3431		<ul> <li>Elections facilities</li> </ul>
3432		<ul> <li>K-12 education facilities</li> </ul>
3433		<ul> <li>Government education facility</li> </ul>
3434		<ul> <li>Military facility</li> </ul>
3435		<ul> <li>National monument &amp; icon</li> </ul>
3436		<ul> <li>Personnel-oriented government facility</li> </ul>
3437		<ul> <li>Service-oriented government facility</li> </ul>
3438		<ul> <li>Government sensor or monitoring facility</li> </ul>
3439		<ul> <li>Government space facility</li> </ul>
3440		<ul> <li>Government storage or preservation facility</li> </ul>
3441	•	Healthcare and public health
3442		<ul> <li>Direct patient healthcare</li> </ul>
3443		<ul> <li>Health information technology</li> </ul>
3444		o Fatality/mortuary services
3445		<ul> <li>Medical materials</li> </ul>
3446		<ul> <li>Laboratories, blood, and pharmaceuticals</li> </ul>
3447		<ul> <li>Public health services</li> </ul>
3448		<ul> <li>Healthcare educational facility</li> </ul>
3449		<ul> <li>Regulatory, oversight, or industry organization</li> </ul>
3450	•	Information technology
3451		<ul> <li>Hardware production</li> </ul>
3452		<ul> <li>Software production</li> </ul>
3453		<ul> <li>Operational support service facility</li> </ul>
3454		o Internet-based content, information, and communications services
3455	•	Nuclear reactors, materials, and waste
3456		<ul> <li>Nuclear reactor facility</li> </ul>
3457		<ul> <li>Nuclear material processing and handling facility</li> </ul>
3458		<ul> <li>Nuclear waste facility</li> </ul>

3459 •	Transp	portation systems
3460	0	Aviation
3461	0	Maritime
3462	0	Freight rail
3463	0	Highway and motor carrier
3464	0	Pipeline
3465	0	Postal and shipping
3466	0	Mass transit
3467 •	Water	and wastewater systems
3468	0	Drinking water
3469	0	Wastewater
3470	0	Regulatory, oversight, or industry organization
3471		

3472	z. Appendix 5: Federal Agencies and Sub-Agencies
3473	Format of list is as follows:
3474	• Agency
3475	o Sub-agency
3476	List
3477	Advisory Council on Historic Preservation (ACHP)
3478	African Development Foundation (ADF)
3479	<ul> <li>American Battle Monuments Commission (ABMC)</li> </ul>
3480	<ul> <li>Appalachian Regional Commission (ARC)</li> </ul>
3481	Armed Forces Retirement Home
3482	Broadcasting Board of Governors (BBG)
3483	<ul> <li>International Broadcasting Bureau</li> </ul>
3484	Central Intelligence Agency (CIA)
3485	Chemical Safety and Hazard Investigation Board (CSHIB)
3486	• Commission of Fine Arts (CFA)
3487	Commission on Civil Rights (CCR)
3488	Commodity Futures Trading Commission (CFTC)
3489	Congressional Budget Office
3490	Consumer Financial Protection Bureau (CFPB)
3491	• Consumer Product Safety Commission (CPSC)
3492	Corporation for National and Community Service (CNCS)
3493	<ul> <li>Office of Information Technology</li> </ul>
3494	Court Services and Offender Supervision Agency (CSOSA)
3495	<ul> <li>Defense Nuclear Facilities Safety Board (DNFSB)</li> </ul>
3496	<ul> <li>Delaware River Basin Commission (DRBC)</li> </ul>
3497	Department of Agriculture (USDA)
3498	Agricultural Marketing Service (AMS)
3499	Agricultural Research Service
3500	<ul> <li>Animal &amp; Plant Health Inspection Service</li> </ul>
3501	<ul> <li>Assistant Secretary for Administration</li> </ul>
3502	<ul> <li>Assistant Secretary for Congressional Relations</li> </ul>
3503	<ul> <li>Chief Financial Officer</li> </ul>
3504	<ul> <li>Chief Information Officer (CIO)</li> </ul>
3505	<ul> <li>Cooperative State Research, Education, and Extension Service</li> </ul>
3506	o Departmental Administration
3507	<ul> <li>Director of Communications</li> </ul>
3508	<ul> <li>Economic Research Service</li> </ul>
3509	<ul> <li>Executive Operations</li> </ul>
3510	o Farm Service Agency
3511	<ul> <li>Food and Nutrition Service</li> </ul>

3512	Food Safety Inspection Service
3512 c	
3514	
3515 c	
	<u> </u>
3517	8
3518	83 ( )
3519	1
3520	5
3521	8
3522	
3523	
3524	
3525	3
3526	,
3527	8
3528	1
<b>3529</b>	
<b>3530</b> G	5
3531	9
3532	J J
3533	Under Secretary for Marketing and Regulatory Programs
3534	Under Secretary for Natural Resources and Environment
3535	Under Secretary for Research Education and Economics
3536	Under Secretary for Rural Development
3537 • Depa	artment of Commerce (DOC)
3538	Bureau of Economic Analysis (BEA)
3539	Bureau of Export Administration
3540	Bureau of Industry and Security
3541	Bureau of the Census
3542	Chief Information Officer (CIO)
3543	DOC-CIRT
3544	Economic Development Administration
3545	Economics and Statistics Administration
3546	FEDWorld
<b>3547</b>	International Trade Administration (ITA)
3548	
3549	No. 11 Co. 1 1 0 T 1 1 OHGT)
3550	N. T. A. C.
<b>3551</b>	
3552	National Oceanic & Atmospheric Administration (NOAA)
<b>3553</b>	No. 17 1 11 C G GITTO
3554	

3555	<ul> <li>National Weather Service</li> </ul>
3556	<ul> <li>Office of Inspector General</li> </ul>
3557	<ul> <li>Office of the Secretary</li> </ul>
3558	<ul> <li>Patent and Trademark Office</li> </ul>
3559	<ul> <li>Technology Administration</li> </ul>
3560	<ul> <li>U.S. Patent and Trademark Office</li> </ul>
3561	• Department of Defense (DOD)
3562	o Air Force (USAF)
3563	<ul> <li>American Forces Press Service</li> </ul>
3564	o Army (USA)
3565	<ul> <li>Chief Information Officer (CIO)</li> </ul>
3566	<ul> <li>Defense Commissary Agency</li> </ul>
3567	<ul> <li>Defense Contract and Audit Agency (DCAA)</li> </ul>
3568	<ul> <li>Defense Finance and Accounting Service (DFAS)</li> </ul>
3569	<ul> <li>Defense Information Systems Agency (DISA)</li> </ul>
3570	<ul> <li>Defense Intelligence Agency (DIA)</li> </ul>
3571	<ul> <li>Defense Logistics Agency (DLA)</li> </ul>
3572	<ul> <li>Defense Security Service</li> </ul>
3573	<ul> <li>Defense Technical Information Center (DTIC)</li> </ul>
3574	<ul> <li>Joint Chiefs of Staff (JCS)</li> </ul>
3575	<ul> <li>Joint Task Force-Global Network Operations (JTF-GNO)</li> </ul>
3576	<ul><li>Marine Corps (USMC)</li></ul>
3577	<ul> <li>Missile Defense Agency (MDA)</li> </ul>
3578	<ul> <li>National Guard</li> </ul>
3579	<ul> <li>National Security Agency (NSA)</li> </ul>
3580	o Navy (USN)
3581	• Department of Education (EDUC)
3582	<ul> <li>Chief Information Officer (CIO)</li> </ul>
3583	<ul> <li>Educational Resources Information Center (ERIC)</li> </ul>
3584	<ul> <li>Federal Student Aid (FSA)</li> </ul>
3585	<ul> <li>National Library of Education (NLE)</li> </ul>
3586	<ul> <li>Office of Educational Technology</li> </ul>
3587	<ul> <li>Office of General Counsel</li> </ul>
3588	<ul> <li>Office of Inspector General</li> </ul>
3589	<ul> <li>Office of Intergovernmental and Interagency Affairs</li> </ul>
3590	<ul> <li>Office of Legislation and Congressional Affairs</li> </ul>
3591	<ul> <li>Office of Management</li> </ul>
3592	<ul> <li>Office of Public Affairs</li> </ul>
3593	<ul> <li>Office of the Chief Financial Officer</li> </ul>
3594	<ul> <li>Office of the Chief Information Officer</li> </ul>
3595	<ul> <li>Office of the Secretary</li> </ul>
3596	• Department of Energy (DOE)
3597	<ul> <li>Ames Laboratory</li> </ul>

3598	0	Argonne National Laboratory (ANL)
3599	0	Assistant Secretary for Congressional and Intergovernmental
3600	0	Assistant Secretary for Environment Safety and Health (ES&H)
3601	0	Assistant Secretary for Environmental Management
3602	0	Assistant Secretary for Fossil Energy
3603	0	Assistant Secretary for Policy and International Affairs
3604	0	Associate Administrator for Facilities and Operations
3605	0	Associate Administrator for Management and Administration
3606	0	Brookhaven National Lab
3607	0	Chief Information Officer (CIO)
3608	0	Computer Incident Advisory Capability (CIAC)
3609	0	Defense Nuclear Facilities Safety Board Liaison
3610	0	Deputy Administrator for Defense Nuclear Nonproliferation
3611	0	Deputy Administrator for Defense Programs
3612	0	Deputy Administrator for Naval Reactors
3613	0	Energy Information Administration
3614	0	Federal Energy Regulatory Commission
3615	0	FermiLab
3616	0	General Counsel
3617	0	Idaho National Labs
3618	0	Lawrence Berkeley National Laboratory
3619	0	Lawrence Livermore National Laboratory
3620	0	Los Alamos National Laboratory
3621	0	Oak Ridge National Labs
3622	0	Office of Civilian Radioactive Waste Management
3623	0	Office of Counterintelligence
3624	0	Office of Economic Impact and Diversity
3625	0	Office of Emergency Operations
3626	0	Office of Hearings and Appeals
3627	0	Office of Independent Oversights and Performance Assurance
3628	0	Office of Intelligence
3629	0	Office of Management Budget and Evaluation/Chief Financial
3630	0	Office of Nuclear Energy Science and Technology
3631	0	Office of Public Affairs
3632	0	Office of Science
3633	0	Office of Security
3634	0	Office of the Inspector General
3635	0	Office of the Secretary
3636	0	Office of Worker and Community Transition
3637	0	Power Marketing Administrations
3638	0	Secretary of Energy Advisory Board
3639	0	Southwestern Power Administration
3640	0	Under Secretary for Energy Science and Environment

3641	0	Under Secretary for Nuclear Security
3642 •	Depart	ement of Health and Human Services (HHS)
3643	0	Administration for Children and Families
3644	0	Administration on Aging
3645	0	Agency for Healthcare Research and Quality (AHCRQ)
3646	0	Agency for Toxic Substances and Disease Registry
3647	0	Centers for Disease Control and Prevention (CDC)
3648	0	Centers for Medicare and Medicaid Services (CMS)
3649	0	Chief Information Officer (CIO)
3650	0	Financial Management Systems
3651	0	Food and Drug Administration (FDA)
3652	0	Health Resources and Services Administration
3653	0	Indian Health Service
3654	0	National Institutes of Health (NIH)
3655	0	Office of Inspector General
3656	0	Office of the Secretary
3657	0	Program Support Center
3658	0	Secure One Communications Center (SOCC)
3659	0	Substance Abuse and Mental Health Services Administration
<b>3660</b> ●	Depart	ement of Homeland Security (DHS)
3661	0	Bureau of Citizenship and Immigration Services
3662	0	Chief Information Officer (CIO)
3663	0	Cybersecurity and Infrastructure Security Agency (CISA)
3664	0	CSIRC
3665	0	Customs & Border Protection
3666	0	Federal Emergency Management Agency (FEMA)
3667	0	Federal Law Enforcement Training Center
3668	0	Federal Protective Service (FPS)
3669	0	Headquarters
3670	0	HSOC
3671	0	Immigration and Customs Enforcement (ICE)
3672	0	Information Analysis Infrastructure Protection (IAIP)
3673	0	National Coordinating Center (NCC Watch)
3674	0	National Infrastructure Coordination Center (NICC)
3675	0	NCSD
3676	0	Office of Immigration Statistics
3677	0	Office of the Inspector General (OIG)
3678	0	Science and Technology Directorate
3679	0	Transportation Security Administration (TSA)
3680	0	United States Coast Guard
3681	0	United States Secret Service
3682 •	Depart	ment of Housing and Urban Development (HUD)
3683	0	Administration

3684	O Chief Financial Officer
3685	<ul> <li>Chief I maneral Officer</li> <li>Chief Information Officer (CIO)</li> </ul>
3686	<ul> <li>Chief Procurement Officer</li> </ul>
3687	<ul> <li>Community Planning and Development</li> </ul>
3688	<ul> <li>Congressional and Intergovernmental Relations</li> </ul>
3689	Enforcement Center
3690	<ul> <li>Federal Housing Enterprise Oversight</li> </ul>
3691	General Counsel
3692	<ul> <li>Government National Mortgage Association (Ginnie Mae)</li> </ul>
3693	<ul> <li>Government National Wortgage Association (Ginnie Wate)</li> <li>Housing and Urban Development Reading Room</li> </ul>
3694	<ul> <li>Inspector General</li> </ul>
3695	<ul> <li>Multifamily Housing Assistance Restructuring</li> </ul>
3696	<ul> <li>Office of Departmental Equal Employment Opportunity</li> </ul>
3697	<ul> <li>Office of Departmental Operations and Coordination</li> </ul>
3698	Office of Healthy Homes and Lead Hazard Control
3699	<ul> <li>Office of the Secretary</li> </ul>
3700	<ul> <li>Policy Development and Research</li> </ul>
3701	<ul> <li>Public Affairs</li> </ul>
3702	<ul> <li>Public and Indian Housing</li> </ul>
3703	Real Estate Assessment Center
	partment of Justice (DOJ)
3705	Antitrust Division (ATR)
3706	<ul> <li>Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)</li> </ul>
3707	Civil Division
3708	<ul> <li>Civil Rights Division</li> </ul>
3709	Community Relations Service
3710	Criminal Division
3711	o DOJCERT
3712	<ul> <li>Drug Enforcement Agency (DEA)</li> </ul>
3713	Environment and Natural Resources Division
3714	<ul> <li>Executive Office for Immigration Review</li> </ul>
3715	<ul> <li>Executive Office for the U.S. Attorneys</li> </ul>
3716	<ul> <li>Executive Office for the U.S. Trustees</li> </ul>
3717	o Federal Bureau of Investigation (FBI)
3718	o Federal Bureau of Prisons
3719	o Inspector General
3720	o Intelligence Policy and Review
3721	o Intergovernmental Affairs
3722	o Justice and Management Division
3723	o Legal Counsel
3724	o Legal Policy
3725	o Legislative Affairs
3726	o National Drug Intelligence Center (NDIC)

o Office of Community Oriented Policing Services Office of Federal Detention Trustee (OFDT) Office of Information & Privacy (OIP) Office of Justice Programs (OJP) Office of Professional Responsibility (OPR) Office of the Associate Attorney General Office of the Attorney General Office of the Deputy Attorney General Office of the Pardon Attorney
<ul> <li>Office of Information &amp; Privacy (OIP)</li> <li>Office of Justice Programs (OJP)</li> <li>Office of Professional Responsibility (OPR)</li> <li>Office of the Associate Attorney General</li> <li>Office of the Attorney General</li> <li>Office of the Deputy Attorney General</li> </ul>
o Office of Justice Programs (OJP) Office of Professional Responsibility (OPR) Office of the Associate Attorney General Office of the Attorney General Office of the Deputy Attorney General
<ul> <li>Office of Professional Responsibility (OPR)</li> <li>Office of the Associate Attorney General</li> <li>Office of the Attorney General</li> <li>Office of the Deputy Attorney General</li> </ul>
<ul> <li>Office of the Associate Attorney General</li> <li>Office of the Attorney General</li> <li>Office of the Deputy Attorney General</li> </ul>
<ul> <li>Office of the Attorney General</li> <li>Office of the Deputy Attorney General</li> </ul>
o Office of the Deputy Attorney General
± • • • • • • • • • • • • • • • • • • •
o Office of the Pardon Attorney
o Office of the Solicitor General
o Public Affairs
3738 o Tax Division
o U.S. National Central Bureau - INTERPOL (USNCB)
o U.S. Parole Commission
o U.S. Trustee Program (USTP)
o United States Marshals Service (USMS)
• Department of Labor (DOL)
o Administration Review Boards (ARB)
o Benefits Review Board (BRB)
o Bureau of International Labor Affairs (ILAB)
o Bureau of Labor Statistics (BLS)
o Center for Faith-Based and Community Initiatives
o Employee Benefit Securities Administrations (EBSA)
o Employee's Compensation Appeals Board (ECAB)
o Employment Standards Administration (ESA)
o Employment Training Administration (ETA)
o Mine Safety Health Administration (MSHA)
o National Mine Health and Safety Academy
o Office of Congressional and Intergovernmental Affairs
o Office of Disability Employment Policy (ODEP)
o Office of Job Corps (OJC)
o Office of Public Affairs (OPA)
o Office of Safety and Health Administration (OSHA)
o Office of Small Business Programs (OSBP)
o Office of the Administrative Law Justices (ALJ)
o Office of the Assistant Secretary for Policy (OASP)
o Office of the Chief Financial Officer (OCFO)
o Office of the Inspector General (OIG)
o Office of the Secretary (OSEC)
o Office of the Solicitor of Labor (SOL)
o Veterans Employment and Training Service (VETS)
o Women's Bureau (WB)
• Department of State (DOS)

2770	_	A animaltymal Foundation and Dygin and Affairs
3770 3771	0	Agricultural Economics and Business Affairs Appellate Review Board
	0	Board of the Foreign Service
3772	0	_
3773	0	Bureau of Diplomatic Security  Chief Information Officer (CIO)
3774	0	Chief Information Officer (CIO) Commissions
3775	0	
3776	0	Coordinator for Counterterrorism
3777	0	Counselor of the Department
3778	0	Country Officers
3779	0	Democracy Human Rights and Labor Bureau
3780	0	Department of State Library
3781	0	Deputy Secretary
3782	0	Examiners for the Foreign Service
3783	0	Executive Secretariat
3784	0	Foreign Service Grievance Board
3785	0	Historian
3786	0	Intelligence and Research
3787	0	Legal Adviser
3788	0	Legislative Affairs
3789	0	NATO (North Atlantic Treaty Organization)
3790	0	Office of the Secretary
3791	0	Office of the United Nations Ambassador
3792	0	Policy Planning Staff
3793	0	Under Secretary for Arms Control and International Security
3794	0	Under Secretary for Global Affairs
3795	0	Under Secretary for Management
3796	0	Under Secretary for Political Affairs
3797	0	Under Secretary for Public Diplomacy and Public Affairs
3798	0	United National Political Affairs
3799	• Depart	tment of the Interior (DOI)
3800	0	Bureau of Indian Affairs
3801	0	Bureau of Land Management
3802	0	Bureau of Reclamation
3803	0	Chief Information Officer (CIO)
3804	0	DOI CIRC
3805	0	Fish and Wildlife Service
3806	0	Minerals Management Service
3807	0	National Business Center
3808	0	National Park Service
3809	0	Office of Hearings and Appeals
3810	0	Office of Surface Mining
3811	0	Office of the Inspector General
3812	0	Office of the Secretary
3012	O	office of the beefetting

3813	C	US Geological Survey
3814	<ul> <li>Depa</li> </ul>	rtment of the Treasury
3815	C	Alcohol and Tobacco Tax and Trade Bureau (TTB)
3816	С	Bureau of Alcohol Tobacco and Firearms (ATF)
3817	C	Bureau of Engraving and Printing
3818	С	Bureau of the Fiscal Service (BFS)
3819	С	Chief Information Officer (CIO)
3820	С	Comptroller of the Currency
3821	С	Executive Office for Asset Forfeiture
3822	С	Federal Law Enforcement Training Center
3823	С	Financial Crimes Enforcement Network
3824	С	Internal Revenue Service (IRS)
3825	С	Office of the Comptroller of the Currency
3826	С	Office of the Inspector General
3827	С	Office of the Secretary
3828	С	Office of Thrift Supervision (OTS)
3829	С	TCSIRC
3830	С	Treasury Headquarters (Treas-HQ)
3831	С	United States Customs Services
3832	С	United States Mint
3833	С	US Federal Civilian Agency
3834	<ul> <li>Deparement</li> </ul>	rtment of Transportation (DOT)
3835	С	Bureau of Transportation Statistics
3836	С	Chief Information Officer (CIO)
3837	С	
3838	C	Federal Highway Administration
3839	C	
3840	C	
3841	C	
3842	C	
3843	С	$\mathcal{E}$
3844	C	1
3845	C	J
3846	С	1 &
3847	С	J 1 1
3848	С	1
3849	C	ı
3850	C	1 /
3851	<ul> <li>Deparement</li> </ul>	rtment of Veterans Affairs
3852	С	1 &
3853	С	$\mathcal{E}$
3854	С	
3855	С	Allied Clinical Services Strategic Healthcare Group

3856	o Audit
3857	<ul> <li>Austin Automation Center</li> </ul>
3858	<ul> <li>Board of Contract Appeals</li> </ul>
3859	<ul> <li>Board of Veterans' Appeals</li> </ul>
3860	o Budget
3861	<ul> <li>Chief Information Officer (CIO)</li> </ul>
3862	<ul> <li>Congressional and Legislative Affairs</li> </ul>
3863	<ul> <li>Deputy Secretary</li> </ul>
3864	<ul> <li>Disadvantaged and Small Business Utilization</li> </ul>
3865	<ul> <li>Diversity Management and Equal Employment Opportunity</li> </ul>
3866	<ul> <li>Emergency Management Strategic Healthcare Group</li> </ul>
3867	<ul> <li>Employee Education</li> </ul>
3868	<ul> <li>Facilities Management</li> </ul>
3869	<ul> <li>Facilities Service</li> </ul>
3870	<ul> <li>General Counsel</li> </ul>
3871	<ul> <li>Geriatrics and Extended Care Strategic Healthcare Group</li> </ul>
3872	<ul> <li>Information and Technology</li> </ul>
3873	<ul> <li>Inspector General</li> </ul>
3874	<ul> <li>Intergovernmental and Public Affairs</li> </ul>
3875	<ul> <li>Law Enforcement and Security</li> </ul>
3876	<ul> <li>Litigation Docket</li> </ul>
3877	<ul> <li>Management</li> </ul>
3878	<ul> <li>National Cemetery Administration</li> </ul>
3879	<ul> <li>Nursing Strategic Healthcare Group</li> </ul>
3880	<ul> <li>Office of Dentistry</li> </ul>
3881	<ul> <li>Office of Investigations</li> </ul>
3882	<ul> <li>Office of the Secretary</li> </ul>
3883	<ul> <li>Patient Care Services</li> </ul>
3884	<ul> <li>Planning and Elution</li> </ul>
3885	<ul> <li>Planning and Policy</li> </ul>
3886	<ul> <li>Policy Office</li> </ul>
3887	<ul> <li>Primary and Ambulatory Care Strategic Healthcare Group</li> </ul>
3888	<ul> <li>Quality and Performance Office</li> </ul>
3889	<ul> <li>Readjustment Counseling Service</li> </ul>
3890	<ul> <li>Rehabilitation Strategic Healthcare Group</li> </ul>
3891	<ul> <li>Research and Development</li> </ul>
3892	<ul> <li>Support Service</li> </ul>
3893	<ul> <li>Telecommunications</li> </ul>
3894	o VACIRC
3895	o VASOC
3896	<ul> <li>Veterans Benefits Administration</li> </ul>
3897	<ul> <li>Veterans Health Administration</li> </ul>
3898	<ul> <li>Environmental Protection Agency (EPA)</li> </ul>

3899	<ul> <li>Equal Employment Opportunity Commission (EEOC)</li> </ul>
3900	• Executive Office of the President (EOP)
3901	<ul> <li>Office of Management and Budget (OMB)</li> </ul>
3902	<ul> <li>United States Trade Representative (USTR)</li> </ul>
3903	<ul> <li>White House</li> </ul>
3904	• Export-Import Bank of the United States (EIIM)
3905	• Fannie Mae (FNMA)
3906	• Farm Credit Administration (FCA)
3907	<ul> <li>Federal Accounting Standards Advisory Board (FASAB)</li> </ul>
3908	<ul> <li>Federal Communications Commission (FCC)</li> </ul>
3909	<ul> <li>Federal Deposit Insurance Corporation (FDIC)</li> </ul>
3910	<ul> <li>Federal Election Commission (FEC)</li> </ul>
3911	<ul> <li>Federal Energy Regulatory Commission (FERC)</li> </ul>
3912	<ul> <li>Federal Housing Finance Agency (FHFA)</li> </ul>
3913	Federal Judiciary
3914	<ul> <li>Administrative Office of the United States Courts</li> </ul>
3915	• Federal Labor Relations Authority (FLRA)
3916	<ul> <li>Federal Maritime Commission (FMC)</li> </ul>
3917	<ul> <li>Federal Mediation and Conciliation Service (FMCS)</li> </ul>
3918	<ul> <li>Federal Mine Safety and Health Review Commission (FMSHRC)</li> </ul>
3919	• Federal Reserve System (FRS)
3920	<ul> <li>Board of Governors</li> </ul>
3921	• Federal Retirement Thrift Investment Board (FRTIB)
3922	<ul> <li>Thrift Savings Plan</li> </ul>
3923	• Federal Trade Commission (FTC)
3924	• Freddie Mac (FHLMC)
3925	General Services Administration (GSA)
3926	Government Printing Office
3927	<ul> <li>Harry S Truman Scholarship Foundation (HTSF)</li> </ul>
3928	Holocaust Memorial Council (HMC)
3929	<ul> <li>House of Representatives</li> </ul>
3930	Independent Agencies
3931	<ul> <li>United States Consumer Product Safety Commission (CPSC)</li> </ul>
3932	<ul> <li>Institute of Museum and Library Services (IMLS)</li> </ul>
3933	• Institute of Peace United States (USIP)
3934	• Inter-American Foundation (IAF)
3935	<ul> <li>International Boundary and Water Commission</li> </ul>
3936	<ul> <li>International Broadcasting Bureau (IBB)</li> </ul>
3937	<ul> <li>International Trade Commission (ITC)</li> </ul>
3938	• ISAC
3939	o Airport

3940	<ul> <li>Chemical</li> </ul>
3941	o Electricity
3942	<ul> <li>Emergency Fire Services</li> </ul>
3943	o Energy
3944	<ul><li>Financial Services (FS)</li></ul>
3945	<ul> <li>Food and Agriculture</li> </ul>
3946	<ul> <li>Information Technology (IT)</li> </ul>
3947	<ul> <li>Maritime</li> </ul>
3948	o Multi-State (MS)
3949	<ul> <li>National Monuments and Icons</li> </ul>
3950	<ul> <li>Postal and Shipping</li> </ul>
3951	<ul> <li>Public Health</li> </ul>
3952	o Real Estate
3953	<ul> <li>Research and Education</li> </ul>
3954	o State CIO
3955	<ul> <li>Surface Transportation</li> </ul>
3956	o Telecom
3957	o Trucking
3958	o Water
3959	<ul> <li>James Madison Memorial Fellowship Foundation (JMMFF)</li> </ul>
3960	<ul> <li>Japan - United States Friendship Commission (JUSFC)</li> </ul>
3961	<ul> <li>Javits-Wagner-O'Day Program (JWOD)</li> </ul>
3962	<ul> <li>Legal Services Command (LSC)</li> </ul>
3963	<ul> <li>Library of Congress</li> </ul>
3964	<ul> <li>Marine Mammal Commission (MMC)</li> </ul>
3965	<ul> <li>Merit Systems Protection Board (MSPB)</li> </ul>
3966	<ul> <li>Millennium Challenge Corporation (MCC)</li> </ul>
3967	<ul> <li>National Aeronautics and Space Administration (NASA)</li> </ul>
3968	o Ames Research Center (ARC)
3969	<ul> <li>Chief Information Officer (CIO)</li> </ul>
3970	<ul> <li>Glenn Research Center (GRC)</li> </ul>
3971	<ul> <li>Goddard Space Flight Center (GSFC)</li> </ul>
3972	<ul> <li>Jet Propulsion Laboratories (JPL)</li> </ul>
3973	<ul> <li>Johnson Space Center (JSC)</li> </ul>
3974	<ul> <li>Kennedy Space Flight Center (KSFC)</li> </ul>
3975	<ul> <li>Langley Research Center (LRC)</li> </ul>
3976	<ul> <li>Marshall Space Flight Center (MSFC)</li> </ul>
3977	o NASIRC
3978	<ul> <li>Stennis Space Center</li> </ul>
3979	<ul> <li>Wallops Flight Facility (WFF)</li> </ul>
3980	<ul> <li>National Archives and Records Administration (NARA)</li> </ul>
3981	<ul> <li>National Capital Planning Commission (NCPC)</li> </ul>

3982	<ul> <li>National Council on Disability (NCD)</li> </ul>
3983	<ul> <li>National Credit Union Administration (NCUA)</li> </ul>
3984	<ul> <li>National Endowment for the Arts</li> </ul>
3985	<ul> <li>National Endowment for the Humanities</li> </ul>
3986	<ul> <li>National Foundation on the Arts and the Humanities (NFAH)</li> </ul>
3987	<ul> <li>National Gallery of Arts (NGA)</li> </ul>
3988	<ul> <li>National Indian Gaming Commission (NIGC)</li> </ul>
3989	National Institute for Literacy
3990	<ul> <li>National Labor Relations Board (NLRB)</li> </ul>
3991	<ul> <li>National Mediation Board (NMB)</li> </ul>
3992	<ul> <li>National Railroad Passenger Corporation (AMTRAK)</li> </ul>
3993	<ul> <li>National Science Foundation (NSF)</li> </ul>
3994	<ul> <li>US Climate Change Science Program (USGCRP)</li> </ul>
3995	<ul> <li>National Transportation Safety Board (NTSB)</li> </ul>
3996	<ul> <li>Neighborhood Reinvestment Corporation (NBRC)</li> </ul>
3997	Nuclear Regulatory Commission (NRC)
3998	<ul> <li>Nuclear Waste Technical Review Board United States (NWTRB)</li> </ul>
3999	<ul> <li>Occupational Safety and Health Administration (OSHA)</li> </ul>
4000	<ul> <li>Occupational Safety and Health Review Commission (OSHRC)</li> </ul>
4001	<ul> <li>Office of Federal Housing Enterprise Oversight (OFHEO)</li> </ul>
4002	• Office of Government Ethics (OGE)
4003	<ul> <li>Office of Navajo &amp; Hopi Indian Relocation</li> </ul>
4004	Office of Personnel Management
4005	<ul> <li>Office of Special Counsel (OSC)</li> </ul>
4006	<ul> <li>Office of the Director of National Intelligence (ODNI)</li> </ul>
4007	<ul> <li>Information Sharing Environment (ISE)</li> </ul>
4008	o Intelligence Advanced Research Projects Activity (IARPA)
4009	<ul> <li>National Counterproliferation Center (NCPC)</li> </ul>
4010	National Counterterrorism Center (NCTC)
4011	o National Intelligence Council (NIC)
4012	o Office of the National Counterintelligence Executive (ONCIX)
4013	Open Source Information System (OSIS)  Representation System (OSIS)
4014	• Peace Corps (PC)
4015	Pension Benefit Guaranty Corporation (PBGC)
4016	Postal Rate Commission (PRC)
4017	Railroad Retirement Board (RRB)
4018	Recovery Accountability and Transparency Board
4019	• Securities and Exchange Commission (SEC)
4020	• Selective Service System (SSS)
4021	Small Business Administration (SBA)
4022	• Smithsonian Institute (SI)

4023	<ul> <li>Social Security Administration (SSA)</li> </ul>
4024	• State Justice Institute (SJI)
4025	<ul> <li>Susquehanna River Basin Commission (SRBC)</li> </ul>
4026	<ul> <li>Tennessee Valley Authority (TVA)</li> </ul>
4027	• U.S. International Development Finance Corporation (DFC)
4028	• U.S. Senate
4029	<ul> <li>U.S. Trade and Development Agency (TDA)</li> </ul>
4030	<ul> <li>United States Agency for International Development (USAID)</li> </ul>
4031	<ul> <li>United States Arms Control and Disarmament Agency (ACDA)</li> </ul>
4032	<ul> <li>United States Congress</li> </ul>
4033	<ul> <li>Government Accountability Office (GAO)</li> </ul>
4034	<ul> <li>United States International Trade Commission (USITC)</li> </ul>
4035	<ul> <li>United States Postal Service (USPS)</li> </ul>
4036	United States Trade and Development Agency
4037	• US-China Economic and Security Review Commission (USCC)
4038	<ul> <li>Voice of America (VOA)</li> </ul>
4039	