Corporation for National and Community Service

NationalService.gov



The Corporation for National and Community Service is committed to implementing and administering a Privacy Policy that protects its employees and other individuals' personally identifiable information (PII). This Breach Notification Form is available to assist in properly documenting a suspected or confirmed privacy breach. Please complete the form in its entirety and return to privacy@cns.gov for processing. Completion of this form does not exclude you from properly notifying individuals impacted or following local state notification procedures.

Breach Reported by:								
Name:			Supervisor:					
Email:			Email:					
Phone:			Phone:					
Agency/Sub-	Agency/Sub-agency/Component:							

Breach Overview:

Summary of the Breach:

Do not include classified information, sensitive information, or any unnecessary PII. Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including:

- a. A description of the parties involved in the breach;
- b. The physical or electronic storage location of the information at risk;
- c. If steps were immediately taken to contain the breach;
- d. Whether the breach is an isolated occurrence or a systematic problem;
- e. Who conducted the investigations of the breach, if applicable; and
- f. Any other pertinent information.

Date and Time of the Breach:	
Location of the Breach:	



Type of Breach:								
Lost Information or Equipment:	Yes	Unauthorized Disclosure: (e.g., email sent to incorrect address, oral or written	Yes					
Lost information of Equipment:	No	disclosure to unauthorized person disclosing degements						
	Yes	Unauthorized Access:	Yes					
Stolen Information or Equipment:	No	No (e.g., an unauthorized employee or contractor accesses information or an information system)						
Unauthorized Equipment:	Yes	Unauthorized Use: (e.g., employee with agency-authorized access to database	Yes					
(e.g., using an unauthorized personal device, server, or email account to store PII)	No	or file accesses and uses information for personal purposes rather than for official purposes)	No					

Storage Medium:									
Laptop or Tablet:	Yes	No	Smartphone:	Yes	No				
Desktop:	Yes	No	Paper files:	Yes	No				
IT System: (e.g., Intranet/Shared Drive)	Yes	No	Oral Disclosure:	Yes	No				
External Storage Device: (e.g., CD, DVD, USB Drive)	Yes	No							
Email: (Provide the relevant email address, the agency e-mail server (e.g., cloud, personal, private))	, and a descriptic	on of the							
Other: (Provide a detailed description of the medium)									

Reported to US-CERT, Law Enforcement, or Congress:								
Reported to US-CERT:			Yes	No				
Reported to Law Enforcement:			Yes	No	If any are yes, complete the following:			
Reported to Congress:			Yes	No				
Name of recipient(s):								
Title of recipient(s):								
Email of recipient(s):								
Phone of recipient(s):								
Agency and Component:								
Date and Time of the Report:								

Number of Individuals and Safeguards:								
Number of individuals potentially affected by the breach:								
Was the information unstructured: (e.g., open fields on a form or survey)	Yes	No						
Was the information encrypted via a NIST-validated method:	Yes	No						
Does a duplicate set of the potentially compromised information exist:	Yes	No						



Additional Information:
Internal breach (e.g., within the agency's network), external, both, or unknown:
What counter measures, if any, were enabled when the breach occurred:
(List all applicable counter measures and whether each one was NIST certified (e.g., hard drive encryption on laptop, encryption of electronic files, password on smartphone)
What steps, if any, have already been taken to mitigate potential harm:
(e.g., calling or sending separate email(s) to recipient(s) of an unauthorized email to request deletion of original email, contacting web publishing to remove unredacted documents from public website)
Do you have knowledge that any information involved in the breach was intentionally stolen or misused:
(If yes, describe the basis for your knowledge and how the information may have been misused (e.g., evidence of identity theft, hacking, adverse
publicity)

Data Elements and Information Types:

Identifying Numbers								
Social Security number	Truncated or Partial Social Security number							
Driver's License Number	License Plate Number							
DEA Registration Number	File/Case ID Number							
Patient ID Number	Health Plan Beneficiary Number							
Student ID Number	Federal Student Aid Number							
Passport number	Alien Registration Number							
DOD ID Number	DOD Benefits Number							
Employee Identification Number	Professional License Number							
Taxpayer Identification Number	Business Taxpayer Identification Number (sole proprietor)							
Credit/Debit Card Number	Business Credit Card Number (sole proprietor)							
Vehicle Identification Number	Business Vehicle Identification Number (sole proprietor)							
Personal Bank Account Number	Business Bank Account Number (sole proprietor)							
Personal Device Identifiers or Serial Numbers	Business device identifiers or serial numbers (sole proprietor)							
Personal Mobile Number	Business Mobile Number (sole proprietor)							



Biographical Information						
Name (including nicknames)		Gender	Race			
Date of Birth (Day, Month, Year)		Ethnicity	Nationality			
Country of Birth		City or County of Birth	Marital Status			
Citizenship		Immigration Status	Religion/Religious Preference			
Home Address		Zip Code	Home Phone or Fax Number			
Spouse Information		Sexual Orientation	Children Information			
Group/Organization Membership		Military Service Information	Mother's Maiden Name			
Business Mailing Address (sole proprietor)		Business Phone or Fax Number (sole proprietor)	Global Positioning System (GPS)/Location Data			
Personal e-mail address		Business e-mail address	Employment Information			
Personal Financial Information (including loan information)		Business Financial Information (including loan information)	Alias (e.g., username, screenname)			
Education Information		Resume or curriculum vitae	Professional/personal references			

Biometrics/Distinguishing Features/Characteristics							
Fingerprints	Vascular scans						
Retina/Iris Scans	Dental Profile	Scars, marks, tattoos					
Hair Color	Eye Color	Height					
Video recording	Photos	Voice/Audio Recording					
DNA Sample or Profile	Signatures	Weight					

Medical/Emergency Information							
Physical Health Information		Mental Health Information		Disability Information			
Workers' Compensation Information		Patient ID Number		Emergency Contact Information			

	Device Information							
(e.	Device settings or preferences .g., security level, sharing options, ngtones)		Cell tower records (e.g., logs, user location, time)		Network communications data			

Specific Information/File Types		
Taxpayer Information/Tax	Law Enforcement Information	Security Clearance/ Background
Return Information		Check Information
Civil/Criminal History	Academic and Professional	Health Information
Information/Police Record	Background Information	
Case files	Personnel Files	Credit History Information

Additional Information

