BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT

X	INITIAL REPORT	Date: (MM/DD/YYYY) 09/09/2022		UPDATED REPORT	Date: (MM/DD/YYYY)		AFTER ACTION REPORT	Date: (MM/DD/YYYY)

1. GENERAL INFORMATION

a. DATE OF BREACH (MM/DD/YYYY)	b. DATE BREACH DISCOVERED (MM/DD/YYYY)	c. DATE REPORTED TO US-CERT (MM/DD/YYYY)	d. US-CERT NUMBER
09/07/2022	09/07/2022		
e. COMPONENT INTERNAL TRACKING NUMBER (If applicable)	**f. BREACH INVOLVED (Click to select)**	**g. TYPE OF BREACH (Click to select)**	**h. CAUSE OF BREACH (Click to select)**
2023-MG-43389	Info dissemination	Compromise	Failure to follow policy

i. COMPONENT (Click to select)	j. OFFICE NAME
DoD Field Activity	Defense Human Resources Activity (DHRA)

POINT OF CONTACT FOR FURTHER INFORMATION:

k. FIRST NAME	l. LAST NAME	m. RANK/GRADE AND TITLE
(b)(6)	(b)(6)	(b)(6)

n. DUTY E-MAIL ADDRESS	o. DUTY TELEPHONE NUMBER
(b)(6)	(b)(6)

MAILING ADDRESS:

p. ADDRESS	q. CITY	r. STATE	s. ZIP CODE
(b)(6)	(b)(6)	(b)(6)	(b)(6)

2.a. DESCRIPTION OF BREACH *(Up to 150 words, bullet format acceptable).* **NOTE: Do NOT include PII or Classified Information.**

A supervisor contacted our time keeping team seeking the last 2 LES slips of a particular employee, stating that the employee's last pay period submission was "significantly uncoordinated." Although the supervisor may have required knowledge of the employee's leave balances, the amount of information available on the LES was significantly more than necessary. Additionally, the leave balance information is available to the supervisor through the time keeping application, DAI. Accessing the information, which is specific to leave balance, would have eliminated the unnecessary exposure of PII to the supervisor.

2.b. ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED *(Up to 150 words, bullet format acceptable).* **NOTE: Do NOT include PII or Classified Information.**

- The supervisor's leadership has instructed the supervisor to permanently delete any copies of the employee's LES.
- The supervisor's leadership will be counseling the individual and taking the necessary HR actions, if appropriate, to ensure such overreach does not occur again.

(b)(6)

3.a. NUMBER OF INDIVIDUALS AFFECTED

(1) Contractors	
(2) DoD Civilian Personnel	1
(3) Military Active Duty Personnel	
(4) Military Family Members	
(5) Military Reservists	
(6) Military Retirees	
(7) National Guard	
(8) Other *(Specify)*:	

b. WERE AFFECTED INDIVIDUALS NOTIFIED? [ ] Yes [X] No

(1) If Yes, were they notified within 10 working days? [ ] Yes [ ] No

(2) If Yes, notification date *(MM/DD/YYYY)*

(3) If Yes, number of individuals notified:

(4) If notification will not be made, explain why, or if number of individuals notified differs from total number of individuals affected, explain why:

This was immediately identified and reported. Additionally, once identified, Supervisor was instructed to permanently delete any copies of the LES. There is limited risk to the impacted individual.

(5) If applicable, was credit monitoring offered? [ ] Yes [ ] No

(6) If Yes, number of individuals offered credit monitoring:

4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH *(X all types that apply)*

[X]	(1) Names	[ ]	(7) Passwords
[X]	(2) Social Security Numbers	[X]	(8) Financial Information*
[ ]	(3) Dates of Birth	[ ]	(9) Other *(Specify)*:
[ ]	(4) Protected Health Information (PHI)		
[ ]	(5) Personal e-mail addresses		
[ ]	(6) Personal home addresses		

*If Financial Information was selected, provide additional detail:

[X] (a) Personal financial information

[ ] (b) Government credit card If yes, was issuing bank notified? [ ] Yes [ ] No

[ ] (c) Other *(Specify)*:

Financial information included TSP contributions and Tax withholdings information.

5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH

[ ] a. PAPER DOCUMENTS/RECORDS *(If selected, provide additional detail)*	[ ] b. EQUIPMENT *(If selected, provide additional detail)*
(1) Paper documents faxed	(1) Location of equipment
(2) Paper documents/records mailed	(2) Equipment disposed of improperly
(3) Paper documents/records disposed of improperly	(3) Equipment owner
(4) Unauthorized disclosure of paper documents/records	(4) Government equipment Data At Rest (DAR) encrypted
(5) Other *(Specify)*:	(5) Government equipment password or PKI/CAC protected
	(6) Personal equipment password protected or commercially encrypted

c. IF EQUIPMENT, NUMBER OF ITEMS INVOLVED

(1) Laptop/Tablet		(4) MP3 player		(7) Flash drive/USB stick/other removable media		*(If Other, Specify)*:
(2) Cell phone		(5) Printer/Copier/Fax/Scanner		(8) External hard drive		
(3) Personal Digital Assistant		(6) Desktop computer		(9) Other		

[ ] d. EMAIL *(If selected, provide additional detail)*	[X] e. INFO DISSEMINATION *(If selected, provide additional detail)*
(1) Email encrypted	(1) Information was posted to the Internet
(2) Email was sent to commercial account *(i.e., .com or .net)*	(2) Information was posted to an intranet *(e.g., SharePoint or Portal)*
(3) Email was sent to other Federal agency	(3) Information was accessible to others without need-to-know on a share drive
(4) Email recipients had a need to know	(4) Information was disclosed verbally
	(5) Recipients had a need to know No

[ ] f. OTHER *(Specify)*:

6.a. TYPE OF INQUIRY *(If applicable) (Click to select) (If Other, specify)*

Internal

b. IMPACT DETERMINATION *(for Component Privacy Official or designee use only) (X one)*

[X] Low [ ] Medium [ ] High

c. ADDITIONAL NOTES *(Up to 150 words, bullet format acceptable)* **NOTE: Do NOT include PII or Classified Information.**

INSTRUCTIONS FOR COMPLETING DD FORM 2959, BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT

Select Initial, Updated, or After Action Report and enter the date.

1. GENERAL INFORMATION.

a. Date of Breach. Enter the date the breach occurred. If the specific date cannot be determined, enter an estimated date and provide further explanation in the notes section of the report.

b. Date Breach Discovered. Enter the date the breach was initially discovered by a DoD employee, military member, or DoD contractor.

c. Date reported to US-CERT. Breaches must be reported to US-CERT within 1 hour of discovery. Enter the date reported to US-CERT.

d. US-CERT Number. Enter the number assigned by US-CERT when the breach was reported.

e. Component Internal Tracking Number (if applicable). If your component uses an internal tracking number, enter the number assigned.

f. Breach Involved (click to select). Select from the drop-down list - Email, Info Dissemination, Paper Records, or Equipment.

g. Type of Breach (click to select). Select from the drop-down list - Theft, Loss, or Compromise.

h. Cause of Breach (click to select). Select from the drop-down list the predominate cause of the breach - Theft, Failure to Follow Policy, Computer Hacking, Social Engineering, Equipment Malfunction, Failure to Safeguard Government Equipment or Information, Improper Security Settings, or Other.

i. - j. Component. Select from the drop-down list. After you select your Component, enter the Office/Name in block 1.j (i.e., if "OSD/JS" is the Component selected, an example of the Office would be "TMA").

k. - s. Point of Contact for Further Information. Enter the requested information for the person to be contacted if DPCLO requires additional details regarding the breach.

2.a. DESCRIPTION OF BREACH (Up to 150 words, bullet format acceptable). Note: Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss or compromise of PII as currently known, including:

- the description of the parties involved in the breach;
- the physical or electronic storage location of the data at risk;
- if steps were immediately taken to contain the breach;
- whether the breach is an isolated incident or a systemic problem;
- who conducted the investigation of the breach; and
- any other pertinent information.

b. ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED (Up to 150 words, bullet format acceptable). Note: Do not include PII or classified information. Summarize steps taken to mitigate actual or potential harm to the individuals affected and the organization. For example, training, disciplinary action, policy development or modification, information systems modifications. List any findings resulting from the investigation of the breach.

3.a. NUMBER OF INDIVIDUALS AFFECTED. For each category of individuals listed, enter the number of individuals affected by the breach. Do not include an individual in more than one category.

b. Were affected individuals notified? Check box "Yes" or "No". If the individuals affected will not receive a formal notification letter about the breach, select "No" and enter an explanation of why the Component determined notification was not necessary in 3.b.(4). If additional space is needed for this justification, continue text in 6.c., Additional Notes.
(1) If affected individuals were notified, were they notified within 10 working days? Check "Yes" or "No".
(2) If the affected individuals will be notified of the breach, provide the date the notification letters will be sent.
(3) - (4) If "Yes", list the number of individuals notified. If the number of individuals notified differs from total number of individuals affected, explain why in 3.b.(4).
(5) Was credit monitoring offered? Select "Yes" or "No".
Note: This is a risk of harm based decision to be made by the DoD Component.
(6) If "Yes", enter the number of individuals offered credit monitoring.

4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH. Select all that apply. If Financial Information is selected, provide additional details.

5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH. Check at least one box from the options given. If you need to use the "Other" option, you must specify other equipment involved.

a. Paper Documents/Records. If you choose Paper Documents/Records, answer each associated question by selecting from the drop-down options.

b. - c. Equipment. If you choose Equipment, answer the associated questions by selecting from the drop-down options. Enter a number in the empty field indicating how many pieces of each type of equipment were involved in the breach. If "Other", you will need to specify what type of equipment was involved.

d. - e. Email and Info Dissemination. If Email or Info Dissemination is selected, choose either "Yes" or "No" for all of the questions.

6.a. TYPE OF INQUIRY. Select the type of inquiry conducted as a result of the breach. If the inquiry type is "Other", please describe.

b. Impact Determination. (Component Privacy Official or designee use only.) Select one: What is the overall risk level associated with this breach? Risk is determined by considering the likelihood that the PII can be accessed by an unauthorized person and assessing the impact to the organization and individual if the PII is misused.

c. Additional Notes. This field can be used to convey additional information.