

REPORTING TO RCERT/ACERT

Report any incident involving the possible compromise of Army Networks to the appropriate Regional Computer Emergency Response Team (RCERT). If analysis conducted by the Army Computer Emergency Response Team (ACERT) confirms possible PII loss, the RCERT notifies the appropriate Unit Information Assurance Officer to initiate PII Loss Reporting IAW information above. The Army FOIA/PA office will provide a copy of all Army PII reports received involving automation equipment to the ACERT Theater Operations Center for situational awareness and analysis.



INDIVIDUAL NOTIFICATION

The organization responsible for safeguarding the PII at the time of the incident must notify the affected individuals. Low/Moderate/High Risk or Harm determinations and the decision whether notifications of individuals is made, rest with the head of the Army Command/Agency where the breach occurred. All determinations of High Risk/Harm require notification. When the actual Army Activity is unknown, by default the responsibility for reporting the incident and notification of affected individuals lies with the originator of the document or information. Notification should be made by an individual at a senior level (i.e., commander/director) to reinforce to impacted individual the seriousness of the incident. A sample notification letter and more information reference the material in this brochure is available at https://www.rmda.army.mil/privacy/docs/ALARACT_050_2009_1.pdf



REPORTING REQUIREMENTS AT-A-GLANCE

- ⇒ US-CERT WITHIN ONE HOUR AT [HTTP://WWW.US-CERT.GOV](http://www.us-cert.gov)
- ⇒ ARMY LEADERSHIP AT PII.REPORTING@US.ARMY.MIL
- ⇒ ARMY FOIA/PA OFFICE WITHIN 24 HOURS AT <https://www.rmda.army.mil/privacy/foia-incidentreport1.asp>
- ⇒ REGIONAL COMPUTER EMERGENCY RESPONSE TEAM (RCERT) & ARMY COMPUTER EMERGENCY RESPONSE TEAM (ACERT) FOR POSSIBLE COMPROMISE OF ARMY NETWORKS.
- ⇒ DETERMINE NATURE OF BREACH AND TYPE BY ASSESSING LOW/MODERATE/HIGH RISK OR HARM
- ⇒ FOR INDIVIDUAL NOTIFICATIONS, SEE SAMPLE NOTIFICATION LETTER AT www.rmda.army.mil.

FREEDOM OF INFORMATION ACT OFFICE
Administrative Services Division
Directorate of Human Resources
US Army Garrison, Presidio of Monterey
373 Patton Avenue
Monterey, CA 93944
(831) 242-6215/6319
pres.asb@conus.army.mil



U.S. ARMY INSTALLATION MANAGEMENT COMMAND

Personally Identifiable Information



Reporting Checklist



REPORTING

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACHES

REPORTING REQUIREMENTS

<u><i>Within One-Hour</i></u>	<u><i>Within 24-Hours</i></u>	<u><i>Following Internal Command Procedures</i></u>
<p>Report all incidents involving the actual or suspected breach/compromise of PII to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery at http://www.us-cert.gov. If computer access is not available, PII incidents can be reported to a 24/7 toll free number at 1-866-606-9580 from the Office of the Administrative Assistant to the Secretary of the Army or US-CERT at 703-235-5110 also monitored 24/7. The individual discovering the incident should directly report incident to meet one hour timeline. Simultaneously, an email should be sent to _____ which notifies Army leadership that an initial report has been submitted. This email should include US-CERT number and a brief synopsis and contact information for the incident.</p>	<p>The individual discovering the breach/compromise, in coordination with the Command/Agency that created the data if known, must report all incidents involving the actual or suspected breach/compromise of PII to the Army Freedom of Information/Privacy Act Office (FOIA/PA) within 24 hours of discovery. The reporting format and submission guidelines are located at https://www.rmda.army.mil/organization/pa-guidance.shtml. Submit updated reports reflecting the results of investigative efforts, remedial action and notification efforts of affected individuals as they become available. The Army FOIA/PA is the centralized office for all Army PII incident reporting, information, and statistics.</p>	<p>Continue to follow existing Internal Command Procedures to notify local command officials. This includes but is not limited to Serious Incident Reports (IMCOM Regulation 190-1), contacting the Army or Regional Computer Emergency Response Team for Network Intrusion Incidents, and notification of credit card company, local law enforcement, Privacy Act Officials and the Public Affairs Office. Internal Command Notifications may not delay the one hour US-CERT or 24 hour Army FOIA/PA office reporting requirements.</p>

DETERMINING THE NATURE OF THE BREACH AND TYPE OF PII INVOLVED

FACTORS	RISK	COMMENTS
a. The name of one or more individuals was released. (A separate notification must be made for each individual affected.)	Low	
b. An individual's name and one or more identifiers were released. ("Identifiers" are any information that relates or is unique to an individual's identity.)	Moderate	
c. A name together with the named person's social security number or together with medical or financial data concerning the individual was released.	High	
d. A password was compromised. (Assess the likelihood of the password being accessible and usable.)	Moderate or High, as applicable	
e. Assess the likelihood of the breach leading to harming the individual affected	Low, Moderate, or High, as applicable	
f. Determine if the data was compromised with or without malicious intent.	Low if without malicious intent / High if malicious	
g. Determine if the breach was caused by a loss of the information (for example, loss of wallet, purse, or laptop).		
h. Determine if the breach was caused by theft (for example, stolen wallet, purse, or laptop).		