DEPARTMENT OF DEFENSE
DEFENSE PRIVACY AND CIVIL LIBERTIES DIVISION
241 18TH STREET SOUTH, SUITE 101
ARLINGTON, VA 22202

FEB 20 2015

MEMORANDUM FOR DoD COMPONENT PRIVACY OFFICERS

SUBJECT: New FY 2015 Annual Federal Information Security Management Act (FISMA) Breach Response and Notification Reporting Requirement

Reference: US Department of Homeland Security, Office of Cybersecurity and Communications, Federal Network Resilience, "FY 2015 Senior Agency Official for Privacy Federal Information Security Management Act Reporting Metrics, v1.0," January 14, 2015

The Department of Homeland Security (DHS) recently published the Fiscal Year 2015 Senior Agency Official for Privacy (SAOP) FISMA Reporting Metrics (Reference). A key component of those changes is the Breach Response and Notification reporting requirements for the FY 2015 Annual SAOP FISMA report.

To ensure DoD complies with this new guidance for the FY 2015 (current) FISMA reporting year, all cyber and non-cyber related breaches will need to be reported in the DoD Component's Senior Agency Official for Privacy FISMA Report due annually in September. The required method for reporting breaches within DoD is the DPCLD Compliance and Reporting Tool (CART). The official breach reporting form is the DD Form 2959, "Breach of Personally Identifiable Information (PII) Report." To facilitate the ease of reporting these new metrics, DoD Components need to be certain they are now tracking the four (4) new breach metrics in CART as each DoD Component will be asked to report on these new metrics in their September 2015 Annual SAOP FISMA report.

The new Breach Response and Notification metrics for the Annual SAOP FISMA Report are:

- Number of confirmed breaches reported by your organization to the U.S. Computer Emergency Readiness Team (US-CERT) during the reporting period.

- Number of confirmed non-cyber related (e.g., paper) breaches experienced by your organization during the reporting period (OMB M-15-01 provided that non-cyber related incidents should be reported to your agency's privacy office and not to US-CERT).

- Number of persons potentially affected by all confirmed breaches, both cyber and non-cyber, during the reporting period (approximate figures if precise figures are not available).

- Number of potentially affected persons who were provided notification about a breach of information experienced by your organization that occurred during the reporting period.

It is important to note that the above metrics use the word "confirmed" for breach reporting to US-CERT and to the agency's privacy office for purposes of the annual FISMA report. This does **not** constitute a change of breach reporting and notification policy in DoD. DoD Components will continue with current DoD reporting and notification practices, but will ensure the paper record breaches are reported in CART per the above metrics.

My point of contract for Annual SAOP FISMA reporting requirements is Mr. John D. Nogan. He can be reached at john.d.nogan.ctr@mail.mil. The point of contact for breach reporting is Ms. Denise Washington who can be reached at denise.f.washington.civ@mail.mil. Both can be reached by phone at (703) 571-0070.

Sincerely,

Samuel P. Jenkins
Acting Chief