Department of Veterans Affairs

Memorandum

Date: March 1, 2019

From: System Owner: Rafael Richards

Subj: System Owner Responsibilities for

To: System Name: VistA Adaptive Maintenance - VA Enterprise Cloud Security
Designated Approving Authority (DAA); Chief Information Security Officer (CISO)

1. As the System Owner, I acknowledge that I have official organizational responsibility for the procurement, development, integration, modification, operation, maintenance, and disposal of information systems in my area of responsibility. In that capacity, I am responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements), and for ensuring compliance with information security requirements.

2. As the focal point for the information system, I serve both as an owner and as the central point of contact between the authorization process and the owners of components of the system to include:

   A. Applications, networking, servers, or workstations;
   B. owners/stewards of information processed, stored, or transmitted by the system; and,
   C. owners of the missions and business functions supported by the system.

3. As the system owner, I confirm my specific responsibilities include:

   A. Informing appropriate organizational officials of the need to conduct the security authorization and ensuring that the necessary resources are available for the effort;
   B. developing the System Security Plan (SSP) in coordination with information owners, the system administrator, the Information System Security Officer (ISSO), the senior agency Information Security Officer (ISO), and functional "end users";
   C. maintaining the SSP and ensuring that the system is deployed and operated according to the agreed-upon security requirements;
   D. developing and implementing the System Test and Evaluation (ST&E) plan;
   E. ensuring that system users and support personnel receive the requisite security training, e.g., instruction in Rules of Behavior;
   F. updating the SSP whenever a significant change occurs;
   G. assisting in the identification, implementation, and assessment of the common security controls;
   H. assembling the authorization package and submitting the package to the Authorizing Official (AO) or the AO's official designated representative for adjudication;
   I. ensuring the accreditation artifacts uploaded into the Governance, Risk and Compliance (GRC) tool are accurate;
   J. deciding who has access to the system and what types of privileges or

access rights are granted;

K. providing the required information system access, information, and documentation to the security control assessor; and,

L. developing and implementing a corrective Plan of Actions and Milestones (POAM) for identified deficiencies with a completion date not to exceed 180 days and to include committed staffing, required funding and list of all dependencies.

X Rafael M. Richards

Digitally signed by Rafael M. Richards
DN: cn=Rafael M. Richards, o=VA, ou=VA, email=rafael.richards@va.gov, c=US
Date: 2019.03.01 13:10:03 -05'00'

System Owner

Name:	Rafael Richards
Title:	Architect, VistA Adaptive Maintenance
Series-Grade:	Title 38
Organization:	Office of Information Governance
Email:	rafael.richards@va.gov
Phone:	202-469-1527
Supervisor:	Charles Hume
Supervisor Email:	charles.hume@va.gov

References:

1. The Federal Information Security Modernization Act of 2014
2. National Institute of Standards and Technology (NIST) Special Publications
    a. 800-18
    b. 800-30
    c. 800-37
    d. 800-39
    e. 800-53
3. Department of Veterans Affairs Handbook 6500