MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Facility-Related Control System Cybersecurity Plan Updates

Cyber vulnerabilities continue to jeopardize critical infrastructure that enables the Department of Defense (DoD) operations. Unsecured control systems can potentially lead to mission failure, operational impacts, and physical damage to critical infrastructure as well as expose connected DoD information networks to risk. Over the past year, we have seen increased activity throughout the Department towards cyber securing mission critical Facility-Related Control Systems (FRCS). Components are, to varying degrees, planning, programming, budgeting, and executing resources to develop relevant cyber hardening and risk reduction plans to detect, mitigate, and recover their systems and information from the advanced, persistent cyber threat.

The purpose of this memorandum is to request updated Component FRCS Cybersecurity Plans that cover Fiscal Years (FY) 2018-2023. To gauge progress, I am also requesting information on accomplishments during FYs 2016-2017. Submissions should prioritize cybersecurity plan completion by the end of FY 2019 on the most critical FRCS including those:


2) That connect to the DoD Information Network, are internet-facing and/or stand-alone, and which require an Authorization to Operate.

Attachment A provides guidance for formulating your FRCS Cybersecurity Plans. Attachment B provides a recommended template. The template may be used for submission, but previous formats are acceptable, if updated to include the new and updated plan requirements. Note that in addition to the previous plan submissions, this data call requires submission of new content. Please submit all FRCS Cyber Plans to my point of contact, Mr. Daryl Haegley, daryl.r.haegley.civ@mail.mil, 571-372-685 by July 31, 2018.

Thank you for your continued support to improve the Department’s FRCS resilience and security posture.

Lucian Niemeyer

Attachments:
As stated
DISTRIBUTION:

ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS, ENERGY AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE NAVY (ENERGY, INSTALLATIONS AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (INSTALLATIONS, ENVIRONMENT AND ENERGY)
DIRECTOR, DEFENSE COMMISSARY AGENCY (INFRASTRUCTURE SUPPORT)
DIRECTOR, DEFENSE LOGISTICS AGENCY (INSTALLATION SUPPORT)
DIRECTOR, MISSILE DEFENSE AGENCY (FACILITIES, MILITARY CONSTRUCTION AND ENVIRONMENTAL LIABILITIES)
DIRECTOR, NATIONAL SECURITY AGENCY (INSTALLATION LOGISTICS)
CHIEF, DEPARTMENT OF DEFENSE EDUCATION ACTIVITY (FACILITIES)
DIRECTOR, DEFENSE HEALTH AGENCY (PORTFOLIO PLANNING AND MANAGEMENT DIVISION)
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (FACILITIES SERVICES DIRECTORATE)

COPY TO:

DOD CHIEF INFORMATION OFFICER
COMPONENT CIOs
JOINT STAFF/J-3/J-6
DEPUTY COMMANDER, US CYBER COMMAND
DEPUTY COMMANDER, STRATEGIC COMMAND
ASSISTANT CHIEF OF STAFF FOR INSTALLATION MANAGEMENT, ARMY
DIRECTOR OF CIVIL ENGINEERS, AIR FORCE
COMMANDER, U.S. ARMY CORPS OF ENGINEERS
COMMANDER, NAVAL FACILITIES ENGINEERING COMMAND
DIRECTOR, SHORE READINESS (OPNAV N46)
DIRECTOR, USACE CRITICAL INFRASTRUCTURE CYBER SECURITY
CHIEF, USACE INSTALLATION SUPPORT DIVISION DIRECTORATE OF MILITARY PROGRAMS
Managing Cyber Risks to Facility-Related Control Systems
FRCS Cybersecurity Plans Guidance

March 31, 2016
Updated February 14, 2018

1 INTRODUCTION

Recent Department of Defense (DoD) instructions and guidance direct owners/operators of Facility-Related Control Systems (FRCS) attached to the DoD Information Network (DoDIN) to account for operational resilience and cybersecurity defense posture. The Office of the Assistant Secretary of Defense for Energy, Installations & Environment (OASD EI&E) intends this FRCS Cybersecurity Plans guidance to be used in conjunction with the FY 2016-FY 2023 FRCS Cyber Plan Status and Funding Template. This is to assist the DoD Components with building and recording control system inventories and to ensure a standard format for review across the Department, in accordance with Reference (h). This guidance and the template are Unclassified. The plans will be FOUO or Classified depending upon the information (Reference (s)).

Managing life-cycle cybersecurity risk, per Reference (e), requires considerable collaboration among control systems stakeholders: installation/facility control engineers and operators; physical security; information network and system security experts; and when applicable, control system vendors and system integrators. Resources for carrying out the DoD’s Risk Management Framework (RMF) and registering control systems are available at the RMF Knowledge Service portal (Reference (i)).

1.1 Purpose

Each DoD Component shall develop an FRCS Cybersecurity Plan (referred to hereafter as the ‘Plan’) that maintains Defense Critical Infrastructure (DCI) in accordance with the authority of DoDD 3020.40 (Reference (p)). Maintaining DCI includes DCI assets or control systems supporting DCI assets, initially focused on securing Defense Critical Assets (DCA) and Tactical Critical Assets (TCA) to achieve an environment which ensures cyber protection of FRCS. Plans should address control systems connected to the DoDIN, systems that are Internet-facing, and systems that are stand-alone. Implementing the FRCS Cybersecurity Plan means that each DoD Component will complete the internal tasks required to identify the goals and resources, with milestones set, to identify, register, and implement cyber security controls on DoD FRCS.

1.2 System Overview

1.2.1 Scope

The scope of the Plan includes all elements of a control system (as shown in Figure 1), such as computer hardware, software, and associated sensors and controllers used to monitor and control infrastructure and facilities (e.g., installation electricity, water, wastewater, natural gas, lighting, building heating and air conditioning equipment, utility control systems, building control