KEY ENTITIES IN THE CUI LANDSCAPE

VERSION 2.0

November 2010: White House issues **EO 13556** establishing a CUI Program.

EXECUTIVE BRANCH MANAGMENT

September 2016: NARA/ISOO issues **32 CFR Part 2002** that sets policy and oversight requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.

POLICY OVERSIGHT

OUSD(I&S) implements the DOD CUI Program and establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DOD in accordance with **DODI 5200.48**.

INFORMATION SYSTEM SECURITY

NIST SP 800-171 identifies the baseline security requirements for industry. CMMC 2.0 is a comprehensive framework that sets priorities for protecting DOD information.

THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Program is administered by DOD OCIO.

CUI PROGRAM IMPLEMENTATION

March 2020: **DODI 5200.48** directs DCSA to administer the DOD CUI program for contractors, assess contractor compliance, develop and maintain threat notifications, educate and train DOD personnel and contractors, provide security assistance, and report Unauthorized Disclosure (UD) of CUI.

DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)

Conducts Defense Industrial Base Cybersecurity assessments in **Clause 253.204-7012.**