

# FISCAM METHODOLOGY AND FISMA METRICS

What You Should Know About Upcoming Changes

# LEARNING OBJECTIVES

- Address changes to the FISCAM methodology and the FISMA metrics
- Discuss the potential impact of these changes
- Answer frequently asked questions

# THE FISCAM METHODOLOGY

- The Federal Information System Controls Audit Manual (FISCAM) presents a methodology for assessing the design, implementation, and operating effectiveness of information system (IS) controls.
- The FISCAM methodology is designed to be applied to a wide variety of IS controls assessments.
- IS controls assessments conducted in accordance with FISCAM may be performed as part of a financial audit, attestation engagement, or performance audit.

# FISCAM 2023 EXPOSURE DRAFT

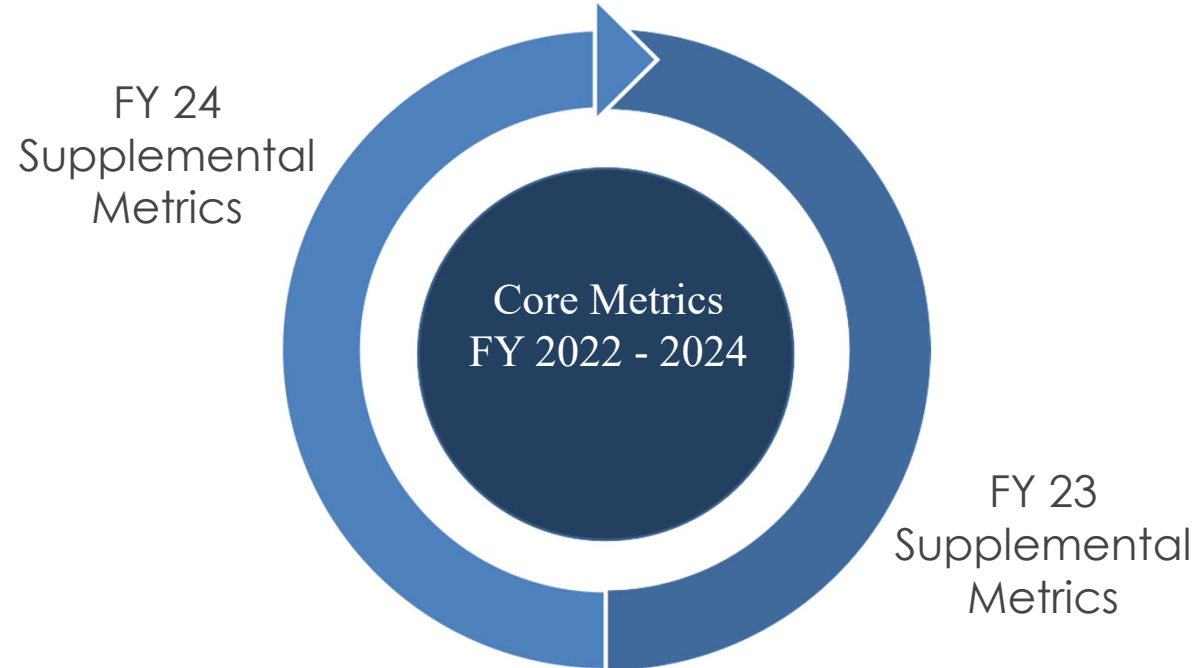
- The changes proposed in the FISCAM 2023 Exposure Draft
  - Enhance FISCAM's format, design, and organization;
  - Update the FISCAM methodology to incorporate changes to auditing standards, clarify auditor requirements, and provide additional guidance on the use of the FISCAM Framework; and
  - Improve the FISCAM Framework.

# FISCAM 2024 REVISION

- This revision of FISCAM has gone through an extensive deliberative process, including focus groups; interviews with internal and external officials, stakeholders, and users; and the collection and incorporation of public comments received on the exposure draft.
- The final product is expected to be issued in Summer 2024.

# IG FISMA REPORTING CYCLE SHIFT

- OMB introduced a cycle shift for IG FISMA reporting in FY 22 – FY 24
  - **Core metrics** – relate to administration priorities and other high-value controls that are evaluated annually
  - **Supplemental metrics** – evaluated on a two-year cycle



# 2025 IG FISMA METRICS DEVELOPMENT PROCESS

- Working group established under the Federal Audit Executive Council's IT subcommittee
- Coordination with federal stakeholders
- Initial thought is to keep the core metrics process intact while tweaking the supplemental metrics

# PLANNED UPDATES TO THE 2025 IG FISMA METRICS

- Incorporation of the Cybersecurity Framework 2.0
  - Governance and supply chain risk management
  - Workforce
  - Consistent terminology
- Metrics modernization
- Alignment with the CIO FISMA metrics
  - Logging, critical software, IPV6 implementation, workforce, high value assets, end of life software, internet of things

# FEDERAL WORK USAGE OF FISCAM & FISMA

## Use of FISCAM in Federal Financial Statement Audits

To determine whether agencies have implemented effective information system controls to initiate, authorize, record, process, summarize, and report financial transactions in the preparation of financial statements.

## FISCAM's revision

- Focuses on the Financial Auditor's areas of audit interest.
- Provides a structure similar to the Financial Audit Manual (FAM).
- Facilitates the assessment of application and general controls within the Financial Auditor's areas of interest.

# FEDERAL WORK USAGE OF FISCAM & FISMA

## FISMA Evaluation Objective

To determine whether agencies have implemented an effective information security program, which may include the protection of financial systems.

## FISMA Overview

- Focuses on both financial and non-financial systems.
- Designed based on the NIST Cybersecurity Framework and maturity model.

# FEDERAL WORK USAGE OF FISCAM & FISMA

- FISCAM focuses on application controls and the general controls that provide a suitable environment to support the effective operation of application controls.
- FISMA emphasizes the maturity level of control processes and the overall effectiveness of the security program.
- Both FISCAM and FISMA reference NIST as a criterion.
- They share approximately 35 NIST controls in common.
- FISMA also incorporates more references to:
  - OMB memos
  - Executive Orders
  - DHS Binding Operational Directives
  - Other criteria

# QUESTIONS & ANSWERS

