COMPARES UAC 1ST READ v103018 TO UAC 2ND READ v120518 [addresses feedback – clean up changes only – not substantive]

15.62 – Protection of Federal Information; FISMA Compliance

v120518

PART 1: PURPOSE

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

As a research institution, New Mexico State University ("university" or "NMSU") seeks and is awarded federal funding, typically subject to information security stipulations. As directed by RPM 2.90, Information Data Security, NMSU administration adopts this rule for the protection of federally funded information as required by law, and as may be required by state and federal agency and regulatory directives pertaining to information security typically incorporated by reference in Grants and Contracts.

This rule does not apply to Criminal Justice Information Services (CJIS) data, whether classified or unclassified. CJIS-related responsibilities are assigned to the ~~University~~NMSU Police Department and are addressed in ARP 16.01, Part 4.

PART 2: DEFINITIONS [rearranged in alpha order]

A. **Chief Information Security Officer (CISO)**: The CISO is the individual responsible for the implementation of security policies and procedures, information security system assessments, and investigation of security violations, and for proposals of changes or new information security policies.

B. **Chief Privacy Officer (CPO)**: The CPO is responsible to interpret FISMA defined information, for the guidance of information security policies, the evaluation of existing information security policies, proposal of new information security policies, or recommendation for changes to existing policies for NMSU. The CPO is the point of contact for security violations and/or suspicious activity, and the subject matter expert on activities under FISMA's purview.

C. **Contract**: A Contract in the context of this rule is a legally binding agreement to provide a product or service for the benefit of the funding agency, in accordance with specific terms and conditions. Contracts provide for payments to the university to cover project costs or to pay a fixed price (in accordance with terms and conditions relating to allowable costs), in exchange for satisfactory completion of the project.

D. **Facility Security Officer (FSO)**: The FSO has an overall individual responsibility for protecting classified information, a contractual obligation to ensure the effective implementation of the security requirements and procedures within a cleared facility involved

in classified projects. The FSO supervises and directs security measures necessary for implementing applicable requirements under the Department of Defense (DoD) National Industrial Security Program (NISP), its operating manual, and related federal requirements for classified information.

E. **Federal Information**: 'Federal information' means information created, collected, processed, maintained, disseminated, or disposed of by or for the federal government, in any medium or form.

~~A.~~F. **FISMA**: The Federal Information Security Management Act of 2002 (FISMA) is a federal law which mandates protection of Federal Information from unauthorized access, use, disclosure, disruption, modification or destruction, in order to provide confidentiality, integrity and availability. The award of Grants, Contracts and other Sponsored Research awards from federal agencies are often conditioned upon compliance with FISMA requirements.

G. **General Facility Security Officer (GFSO)**: The GFSO is responsible for ensuring physical security of facilities as required by federal requirements such as those required by the U.S. Department of Defense and other federal agencies for controlled unclassified information or requiring other physical safeguards.

H. **Grant**: A Grant is an agreement to accomplish something for the public good in exchange for money, property, or services. Federal agencies typically use contractually binding grant agreements for the award of Research funds to universities.

~~B.~~I. **NIST**: The National Institute for Standards and Technology (NIST) is tasked with establishing and codifying the standards to support FISMA. These standards are defined in NIST Special Publications.

J. **NMSU Entity**: sometimes also referred to as "unit", is a general term which may refer to a college, a department or any other individual administrative unit within the NMSU System, including but not limited to agricultural experiment stations.

1. NIST Special Publication 800-53 details the required technical control requirements for classified information and systems.

2. NIST Special Publication 800-171 details the required technical control requirements for protecting controlled unclassified information in Nonfederal Information Systems and Organizations.

~~C.~~A. ~~**Research**: Research as used in this rule is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. *See* 45 CFR 164.501.~~

~~D.~~A. ~~**Grant**: A Grant is an agreement to accomplish something for the public good in exchange for money, property, or services. Federal agencies typically use contractually binding grant agreements for the award of Research funds to universities.~~

~~E.~~A. ~~**Contract**: A Contract in the context of this rule is a legally binding agreement to provide a product or service for the benefit of the funding agency, in accordance with specific terms~~

~~and conditions. Contracts provide for payments to the university to cover project costs or to pay a fixed price (in accordance with terms and conditions relating to allowable costs), in exchange for satisfactory completion of the project.~~

~~F.~~A. ~~**Sponsored Research**: All Research and development activities that are sponsored by federal or other agencies and organizations. This term includes activities involving the training of individuals in Research techniques (commonly called Research training) where such activities utilize the same facilities as other Research and development activities and where such activities are not included in the instruction function.~~

~~G.~~K. **Principal Investigator (PI)**: The PI is the individual responsible for the intellectual direction of a Research project and the training of graduate students. This responsibility includes the conduct of the project, fiscal and administrative accountability, and adherence to the requirements of all relevant laws, regulations, policies, procedures and agreements. If a project has multiple investigators (lead Principal Investigator and co-principal investigators), they shall share the responsibility and accountability for leading and directing the project, both intellectually and logistically. *See* **ARP 11.20 – Responsibilities and Accountability for Sponsored Project Awards**.

L. **Research**: Research as used in this rule is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. *See* 45 CFR 164.501.

M. **Sponsored Research**: All Research and development activities that are sponsored by federal or other agencies and organizations. This term includes activities involving the training of individuals in Research techniques (commonly called Research training) where such activities utilize the same facilities as other Research and development activities and where such activities are not included in the instruction function.

~~H.~~A. ~~**Federal Information**: 'Federal information' means information created, collected, processed, maintained, disseminated, or disposed of by or for the federal government, in any medium or form.~~

~~I.~~A. ~~**Chief Privacy Officer (CPO)**: The CPO is responsible to interpret FISMA defined information, for the guidance of information security policies, the evaluation of existing information security policies, proposal of new information security policies, or recommendation for changes to existing policies for NMSU. The CPO is the point of contact for security violations and/or suspicious activity, and the subject matter expert on activities under FISMA's purview.~~

~~J.~~A. ~~**Chief Information Security Officer (CISO)**: The CISO is the individual responsible for the implementation of security policies and procedures, information security system assessments, and investigation of security violations, and for proposals of changes or new information security policies.~~

~~K.~~A. ~~**General Facility Security Officer (GFSO)**: The GFSO is responsible for ensuring physical security of facilities as required by federal requirements such as those required by the U.S. Department of Defense and other federal agencies for controlled unclassified information or requiring other physical safeguards.~~

~~L.~~A. ~~**Facility Security Officer (FSO)**: The FSO has an overall individual responsibility for protecting classified information, a contractual obligation to ensure the effective implementation of the security requirements and procedures within a cleared facility involved in classified projects. The FSO supervises and directs security measures necessary for implementing applicable requirements under the Department of Defense (DoD) National Industrial Security Program (NISP), its operating manual, and related federal requirements for classified information.~~

~~M.~~A. ~~**NMSU Entity**: sometimes also referred to as "unit", is a general term which may refer to a college, a department or any other individual administrative unit within the NMSU System, including but not limited to agricultural experiment stations.~~

PART 3: FISMA COMPLIANCE AT NMSU

A. NMSU entities awarded funding pursuant to a Grant, Contract, or other award with information security stipulations must comply with FISMA requirements.

B. Administrative support units involved in the administration of any Grant, Contract or award with FISMA stipulations must comply with FISMA requirements. **Such units include and are not limited to**:

1. Information Technology Services
2. Research Administration Services
3. Office of Research Computing
4. Sponsored Projects Accounting

PART 4: FISMA REQUIREMENTS

The National Institute of Standards for Technology (NIST) defines nine general steps for FISMA compliance:

A. Categorize the information to be protected;

B. Select minimum baseline controls;

C. Refine controls using a risk assessment procedure;

D. Document the controls in the system security plan;

E. Implement security controls in appropriate information systems;

F. Assess the effectiveness of the security controls once they have been implemented;

G. Determine agency-level risk to the mission or business case;

H. Authorize the information system for processing; and

I. Monitor the security controls on a continuous basis.

Special Publications (SPs) from NIST such as (NIST SP 800-171) must be used as a guide to accomplish the above steps and to document compliance with FISMA.

PART 5: DUTIES – ROLES AND RESPONSIBILITIES

NMSU designates the Information Technology Compliance Officer as the Chief Privacy Officer (CPO) to coordinate FISMA compliance at all NMSU campuses. This position may perform other tasks and duties on behalf of the university. The CPO is responsible for facilitating compliance with this rule by developing, implementing and maintaining a university system wide FISMA Compliance Program, to include the dissemination of FISMA compliance training and other resources and guidance to the university community. To ensure comprehensive coverage of the program, the CPO should collaborate and coordinate efforts with the NMSU entities and officials listed below and others as appropriate, as well as report progress and issues to the university's Compliance Oversight Committee.

A. **Chief Privacy Officer (CPO)**: The CPO will is responsible for privacy matters related to FISMA as well as ensuring the proper development and implementation of relevant rules and procedures.

B. **Chief Information Security Officer (CISO)**: The CISO will ensure and guide the implementation of technical information security controls in collaboration with the CPO.

~~The~~

C. **General Facility Security Officer (GFSO)**: The GFSO is responsible for ensuring physical security of facilities as required by federal requirements relating to controlled unclassified information or other contractual required physical safeguards.

D. **Facility Security Officer (FSO)**: The FSO is responsible for ensuring physical security of facilities as required by federal requirements and provide guidance on the implementation of physical safeguards relating to classified information.

E. **Research Administration Services (RAS)**: RAS is responsible to maintain a log or other recordkeeping system for those Grants and Contracts which impose requirements on the institution relating to information security, and shall send a notification directly to the CPO and other authorized personnel about the provision(s).

F. **Office of Research Computing:** The Office of Research Computing will work with ~~CPO, OGC,~~the Chief Privacy Officer, Research Administration Services, Sponsored Projects Accounting ~~SPA~~ and others to implement technical or other controls for purposes of FISMA compliance.

G. **Principal Investigator(s~~) will operate and conduct~~):** All Principal Investigators are responsible for operating and conducting their Research or work in a FISMA compliant manner.

~~PART 6: DATA BREACH NOTIFICATION, REPORTING AND HANDLING~~PROTOCOLS

A. All NMSU employees, students or other affiliates upon becoming aware of the potential for private data to be compromised or any type of data breach relating to Federal Information, must report such incidents to the CPO. **The CPO will**:

1. Communicate to NMSU senior officials regarding reported data compromises and breaches;

2. Investigate, document and manage reported incidents in collaboration with General Counsel, Human Resources and other ~~University~~university departments as appropriate;

3. Submit timely notices about data breaches, as required by the various federal agencies, and as required by FISMA or as per the Grant or Contract agreement;

4. Notify affected individuals in collaboration with University Communications; and

5. Retain appropriate documentation for each reported data breach/incident.

PART 7: FISMA TRAINING REQUIREMENTS

Supervisors will arrange for faculty, including affiliated faculty, staff or others authorized to access Federal Information to receive training about this rule and job duties relating to FISMA compliance. With the leadership and guidance from the CPO, the NMSU entities responsible for administration of a Grant or Contract must facilitate such training prior to an employee or other authorized individual commencing work pursuant to the Grant or Contract, and periodically thereafter. One mechanism for delivery of the training may be to invoke the authority of the provost and/or assistant vice president of Human Resource Services to mandate the training pursuant to **ARP 6.89 – Mandatory Employee Training; Professional Development Opportunities**. Official training logs and certificates will be kept in the **Training Central** system maintained by Human Resource Services, **Center for Learning and Professional Development**.