



Department of Energy
Washington, DC 20585

September 10, 2013

MEMORANDUM FOR INGRID KOLB
DIRECTOR, OFFICE OF MANAGEMENT

THROUGH: KEVIN T. HAGERTY
DIRECTOR, OFFICE OF INFORMATION RESOURCES

FROM: ROBERT F. BRESE
CHIEF INFORMATION OFFICER

JM CHRONOLOGY
JM RECEIVED 9/18/13
OUT FOR REVIEW 9/23/13
DRB DISCUSSION 10/3/13

SUBJECT: Notice of Intent to Develop DOE Order ~~2XX-X~~, *Mobile Technology Management* 203.2

PURPOSE: The mobile technology environment is rapidly evolving to leverage increasingly flexible devices and platforms in support of employees performing work anytime, anywhere, and on devices of their choice. While this flexibility is consistent with federal initiatives such as promotion of telework and the Department of Energy (DOE) IT Modernization Strategy it can introduce additional risks to the DOE technology environment. It is essential that Departmental directives and programmatic guidance and procedures evolve along with the changing environment to ensure that DOE's security posture is not compromised. This directive will ensure that federal organizations and employees within the Department can use mobile technology to support mission requirements in a safe and secure manner.

JUSTIFICATION: The intent of this proposed directive is to establish a framework and requirements for management of mobile technology that identifies both permitted and prohibited mobile technologies and practices within the DOE federal IT. There are no current consensuses or other standards specific to mobile technology which can be used in place of this directive. However, there are numerous legal requirements and national IT standards that are applicable to mobile technology and will be considered during the development of this directive.

This directive will apply to all DOE federal employees. Contractor use and management of mobile technology within the DOE environment will be governed by contract requirements and/or connection agreements with DOE elements.

The Office of the Chief Information Officer (OCIO) will develop this directive through an Integrated Project Team comprised of subject matter experts from across the DOE federal and contractor community. This directive will be fully aligned with existing information



technology management and cybersecurity directives and will support the objectives of the DOE telework directive. There are no anticipated impacts on these existing directives.

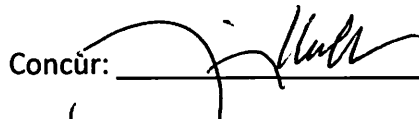
IMPACT: The proposed directive does not duplicate existing laws, regulations or national standards and it does not create undue burden on the Department.

A cross functional assessment team comprised of representatives from NNSA, EM, SC, EE, NE, IM, PMAs, GC, CF, MA, and a variety of Labs and field locations developed the attached Risk Identification and Assessment including risks, policy gaps, and mitigating techniques to address risks related to mobile technology use. The analysis supports the need to establish this proposed directive that will ensure that DOE federal employees can use mobile technology to support performance of mission requirements in a safe and secure manner. This is consistent with legislative and Administration goals related to telework and supports increased productivity of employees on travel or otherwise away from their desks.

The directive will require that all DOE organizations establish guidelines and procedures to ensure that federal employees are adhering to DOE policy. There will be costs associated with this oversight, however, if integrated with existing IT management and cybersecurity oversight processes the additional costs for mobile technology management should be nominal.

WRITER: Helen McBride, 202-586-7549.

OPI/OPI CONTACT: Office of the Chief Information Officer, TheAnne Gordon, 201-586-3705.

Concur:  Nonconcur: _____ Date: 11-21-13

5. The CIO committed to avoiding duplication with other orders (e.g. HSS order).
- Also, the CIO committed to ^{continuing to} engaging with the labs in the development of the order

Risk Identification and Assessment

Subsystem Title or Section within Subsystem

Risk	Probability	Impact	Risk Level
People			
1. Opportunity to increase employee convenience and satisfaction with technology support by enabling use of mobile technology	likely	medium	significant
Mission			
2. Risk of negatively impacting mission accomplishment due to mobile technology use	possible	low	moderate
3. Opportunity to enhance and support agency telework goals by encouraging use of mobile technology	likely	medium	significant
Assets			
4. Risk of damaging the DOE environment by introducing malware and viruses through the use of inadequately secured mobile technology	certain	medium	extreme
Financial			
5. Risk of agency legal liability due to mobile technology use	possible	medium	significant
Customer and Public Trust			
6. Risk of erosion of public trust/confidence in DOE if a highly publicized breach of DOE systems occurs due to use of mobile technology	possible	medium	significant

Gap Analysis of Existing Risks and Controls

Laws	•
External Guidance	<ul style="list-style-type: none"> Office of Management and Budget Digital Government Strategy Draft Government Mobile Security Baseline (in draft as of May 2013)
DOE Regulation	•
DOE Orders	<ul style="list-style-type: none"> DOE Order 205.1B, DOE Cyber Security Program DOE Order 206.1, DOE Privacy Program DOE Order 243.1B, Records Management Program
Contract Controls	•
External Assessments	•

Risk Mitigation Techniques

Risk Assessment for DOE Order 2XX.X, Mobile Technology Management					
Risk/Opportunity	Risk Level	Potential Cost/Benefit	External Control(s)	Proposed Mitigation Technique	Internal Control (if needed)
Opportunity to increase employee convenience and satisfaction with technology support by enabling use of mobile technology	significant	Intangible—improved employee satisfaction	NA	Monitoring	Employee satisfaction gains tracked via management oversight of employee performance
Risk of negatively impacting mission accomplishment due to mobile technology use	moderate	Cost of lost productivity due to misuse of mobile technology	None	Monitoring	Establishes a requirement for program-level oversight processes to ensure appropriate productivity during use of mobile technology
Opportunity to enhance and support agency telework goals by encouraging use of mobile technology	significant	Anticipated productivity gains via increased use of telework	NA	Monitoring	Performance gains tracked via management oversight of employee performance
Risk of damaging the DOE environment by introducing malware and viruses through the use of inadequately secured mobile technology	extreme	Cost of remediation of DOE environment due to damage introduced by mobile technology	None	Mitigation	Establishes a requirement for program-level oversight processes for mobile technology security
Risk of agency legal liability due to mobile technology use	significant	Cost of lawsuits due to mobile technology loss or information breaches	None	Mitigation	Establishes a requirement for program-level oversight processes for mobile technology use
Risk of erosion of public trust/confidence in DOE if a highly publicized breach of DOE systems occurs due to use of mobile technology	significant	Damage to DOE's credibility if sensitive or PII information is lost	None	Mitigation	Establishes a requirement for program-level oversight processes for mobile technology use