ADDENDUM TO
STATE OF MARYLAND PURCHASES
ISSUED UNDER
STATE CONTRACT NO. 060B2490021-2015.

This addendum is applicable to each purchase order that is subject to the State of Maryland's contract number 060B2490021-2015. The contract is the result of the State of Maryland's Request For Proposal ("RFP") for Commercial-Off-the-Shelf ("COTS") Software RFP Project No. 060B2490021-2015.

I. Section 508 Compliance Policy. The Parties agree that the State's Section 508 Compliance Policy is clarified as follows:

> "Contractor's Products are developed using Section 508 standards and substantially comply with the current guidelines. Contractor reports the accessibility of its Products, including accessibility exceptions, on its Voluntary Product Accessibility Templates (VPATs). Information about specific Products and Contractor's VPATs are available at http://www.esri.com/legal/section508/swguide.html. However, it should be noted that Contractor's Products are comprised of geographic information system (GIS) technology that captures, manages, and analyzes visual data through digital maps. Digital maps and GIS technology are inherently visual/graphical and may not have equivalent access in all cases."

II. Security Policies. The Parties agree that the State's security policies are generally not applicable to Esri's COTS Software, and where relevant, shall apply only a case-by-case, order-by-order basis as negotiated by the Parties.

Environmental Systems Research Institute, Inc. (Esri)
Corporate Security Polices
11/20/15

NOTE: WHILE CLOUD PRODUCTS (SaaS / Esri Online Services) SHALL NOT BE PROVIDED UNDER THE MASTER CONTRACT, "CLOUD PRODUCT" INFORMATION IS SET FORTH HEREIN TO MAINTAIN THE CONTINUITY OF ESRI'S CORPORATE SECURITY POLICIES.

On-Premises Products. To meet the requirements of RFP 060B2490021-2015, Section 2.3 – COTS Software, Esri is offering a full suite Esri software "on premises" products to be deployed onto the State of Maryland IT systems. These include ArcGIS for Desktop, ArcGIS for Server, ArcGIS Pro, Portal for ArcGIS and the many extensions available for these products. As described here: deployment model, these products depend on and make use of the customer IT security and infrastructure upon which these products are deployed. In addition, the security and infrastructure layers for these products are the responsibility of the customer. Customers are provided with all the configuration capabilities, documentation and guidelines to implement Esri products securely. An example of these guidelines is here: Securing ArcGIS Server.

Cloud Product. To meet the requirements of RFP 060B2490021-2015, Section 2.3 – COTS Software, Esri is offering ArcGIS Online. ArcGIS Online has received a Federal Agency Production System Security Accreditation. Specifically, ArcGIS Online has been granted Federal Information Security Management Act of 2002 (FISMA) Low Authorization to Operate (ATO) by the USDA. This empowers ArcGIS Online users (including the State of Maryland, under this effort) to securely create interactive web maps to share with whomever they choose, whether it's a specific group, an organization, or the public. FISMA Low controls align with controls provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53. In addition, many security concerns of non-Federal customers are addressed by the ArcGIS Online ATO.

With regard to the applicability of referenced DoIT policies in RFP Section 18.17.1 to ArcGIS Online and Compliance of ArcGIS Online to Applicable Policies: See Table 1.

Table 1: Applicability of State of Maryland DoIT Policies to ArcGIS Online and Compliance of ArcGIS Online to Applicable Policies.

DoIT Document	Length	Document Summary	Assessment WRT ArcGIS Online

DoIT Security Policy	45 pgs.	Direction to Agencies from DoIT to implement protections in accordance with NIST SP 800-53 r3, FIPS 199 and FISMA. Outline follows the NIST SP 800-53 control family divisions.	**ArcGIS Online Complies:** … has a FISMA Low ATO and FISMA controls align with NIST SP 800-53.
CSET Fact Sheet	1 pg.	Maryland DoIT is directing that the CSET (Cyber Security Evaluation Tool), a DHS product, be used for assessing security posture of Agency cyber systems and networks.	**Not Applicable to ArcGIS Online:** … not an Agency System
CRR Fact Sheet	1 pg.	Maryland DoIT is directing that a CRR (Cyber Resilience Review), a DHS process, be used for assessing security posture of Agency cyber systems and networks.	**Not Applicable to ArcGIS Online:** … not an Agency System
IT Security Plan Template	113 pgs.	Template, guidelines and instructions for Agencies to create their Agency-specific Information Technology Security Plans (ITSPs).	**Not Applicable to ArcGIS Online:** … Agencies are responsible for this activity.
Mobile Device Security Policy	2 pgs.	Relates to protection of Maryland-owned Mobile IT devices.	**Not Applicable to ArcGIS Online:** … not a Mobile IT device.
Auto. Email Forwarding	2 pgs.	Relates to restrictions regarding automatic forwarding of State of Maryland email.	**Not Applicable to ArcGIS Online:** … not an email system.
Standards for Security Categorization of Information Systems	3 pgs.	Provides guidelines to categorize the security levels of info. systems based on Confidentially/ Integrity/ Availability FISMA/FIPS 199 Security Objectives.	**Not Applicable to ArcGIS Online:** … Agencies are responsible for this categorization activity.
IT Security Certification & Accreditation Guidelines	20 pgs.	Describes the State of Maryland IT C&A process for Agency systems as a 4 phased activity – Definition, Verification, Validation and Post-Accreditation.	**Not Applicable to ArcGIS Online:** … C&A for systems at Agencies.
Firewall Policies	2 pgs.	Firewall Policies for Agency networks – Platform, Physical Security, Configuration, External Connections, Change Control, Logging and Enforcement.	**Not Applicable to ArcGIS Online:** … Agencies are responsible for these Firewall policies.
Publicly Accessible Systems Policy	2 pgs.	Policies related to public-facing IT systems for State of Maryland agencies.	**Not Applicable to ArcGIS Online:** … by itself ArcGIS Online is not a Public-facing Agency System. (However, note Implementation Services comments (See Table 2)).
Password Policy	3 pgs.	Policy for IT systems passwords for State of Maryland agencies.	**Not Applicable to ArcGIS Online:** … not a State of Maryland IT system.
Remote Access Policy	2 pgs.	Policy for remote connections to DoIT systems for State of Maryland agencies.	**Not Applicable to ArcGIS Online:** … by itself ArcGIS does not implement remote access. (However, note Implementation Services comments (See Table 2)).
Wireless Communication Policy	2 pgs.	Policy for wireless communications to DoIT systems for State of Maryland agencies.	**Not Applicable to ArcGIS Online:** … not a wireless communication technology.

Acknowledge-ment of DoIT Electronic Communications Policy	1 pg.	Form for user of Agency's or State's electronic communications systems. Relevant to Esri employees on-site during the installation process.	**Not Applicable to ArcGIS Online:** … not COTS product requirement. (However, will be relevant to Esri employees on-site during the installation process. (See Table 2)).
Email Encryption Policy	1 pg.	Relates to encryption of emails.	**Not Applicable to ArcGIS Online:** … not an email system.
Incident Report Form	1 pg.	PDF form for reporting IT security incidents to service.desk@maryland.gov	**Not Applicable to ArcGIS Online:** … not COTS product requirement. (However, will be relevant to Esri employees on-site during the installation process. (See Table 2)).

18.17. Security Requirements and Incident Response

18.17.1. The Contractor agrees to abide by all applicable federal, State and local laws concerning information security

- **Applicability to Esri COTS products and Esri Implementation and Training Services.**
  - **Compliance: Esri Complies.**

and comply with current State and Department of Information Technology information security policy, currently found at http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf.

- **Applicability to Esri COTS products and Esri Implementation and Training Services.**
  - **Compliance: See Table 1 and Table 2.**

Contractor shall limit access to and possession of Sensitive Data to only employees whose responsibilities reasonably require such access or possession and shall train such employees on the Confidentiality obligations set forth herein.

- **Applicability to Esri Implementation and Training Services.**
  - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.2. The Contractor agrees to notify the Department when any Contractor system that may access, process, or store State data or Work Product is subject to unintended access or attack. Unintended access or attack includes compromise by a computer malware, malicious search engine, credential compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.

- **Applicability to Esri Implementation and Training Services.**
  - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.3. The Contractor further agrees to notify the Department within twenty-four (24) hours of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the Contract Manager, Department chief information officer and Department chief information security officer.

- **Applicability to Esri Implementation and Training Services.**
  - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.4. The Contractor agrees to notify the Department within two (2) hours if there is a threat to Contractor's product as it pertains to the use, disclosure, and security of the State's data.

- **Applicability to Esri Implementation and Training Services.**
    - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.5. If an unauthorized use or disclosure of any Sensitive Data occurs, the Contractor must provide written notice to the Department within one (1) business day after Contractor's discovery of such use or disclosure and thereafter all information the requests concerning such unauthorized use or disclosure.

- **Applicability to Esri Implementation and Training Services.**
    - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.6. The Contractor, within one day of discovery, shall report to the Department any improper or non-authorized use or disclosure of Sensitive Data. Contractor's report shall identify:

(a) the nature of the unauthorized use or disclosure;
(b) the Sensitive Data used or disclosed,
(c) who made the unauthorized use or received the unauthorized disclosure;
(d) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and
(e) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
(f) The Contractor shall provide such other information, including a written report, as reasonably requested by the State.

- **Applicability to Esri Implementation and Training Services.**
    - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.7. The Contractor shall protect Sensitive Data according to a written security policy no less rigorous than that of the State, and shall supply a copy of such policy to the State for validation. The Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Sensitive Data or other event requiring notification and, should an event occur that triggers an obligation to provide such notification, the Contractor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State and its officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.

- **Applicability to Esri Implementation and Training Services.**
    - **Compliance: Esri Complies. Under current scope, Esri will be conducting installation and training on-site at State of Maryland facilities. Esri will not store any State data or Work Products on Esri IT systems.**

18.17.8. This Section 18.17 shall survive expiration or termination of this Contract.

- **Applicability to Esri COTS products and Esri Implementation and Training Services.**
    - **Compliance: Esri Complies.**

With regard to the applicability of referenced DoIT policies in RFP Section 18.17.1 to Implementation and Training Services and Compliance of the Provision of Services to Applicable Policies: See Table 2.

Table 2: Applicability of State of Maryland DoIT Policies to Implementation and Training Services and Compliance of the Provision of Services to Applicable Policies.

DoIT Document	Length	Document Summary	Assessment WRT Implementation and Training Services
DoIT Security Policy	45 pgs.	Direction to Agencies from DoIT to implement protections in accordance with NIST SP 800-53 r3, FIPS 199 and FISMA. Outline follows the NIST SP 800-53 control family divisions.	**Esri Complies:** … with NIST SP 800-53 controls relevant to personnel security, and personnel training, specifically, control groups: AT, IR, and PS.

CSET Fact Sheet	1 pg.	Maryland DoIT is directing that the CSET (Cyber Security Evaluation Tool), a DHS product, be used for assessing security posture of Agency cyber systems and networks.	**Not Applicable to Esri Implementation and Training Services:** … not a service to be provided by Esri.
CRR Fact Sheet	1 pg.	Maryland DoIT is directing that a CRR (Cyber Resilience Review), a DHS process, be used for assessing security posture of Agency cyber systems and networks.	**Not Applicable to Esri Implementation and Training Services:** … not a service to be provided by Esri.
IT Security Plan Template	113 pgs.	Template, guidelines and instructions for Agencies to create their Agency-specific Information Technology Security Plans (ITSPs).	**Not Applicable to Esri Implementation and Training Services:** … not a service to be provided by Esri.
Mobile Device Security Policy	2 pgs.	Relates to protection of Maryland-owned Mobile IT devices.	**Not Applicable to Esri Implementation and Training Services:** … Esri staff will not have Maryland-owned Mobile IT devices.
Auto. Email Forwarding	2 pgs.	Relates to restrictions regarding automatic forwarding of State of Maryland email.	**Not Applicable to Esri Implementation and Training Services:** … Esri staff will not have State of Maryland email accounts.
Standards for Security Categorization of Information Systems	3 pgs.	Provides guidelines to categorize the security levels of info. systems based on Confidentially/ Integrity/ Availability FISMA/FIPS 199 Security Objectives.	**Not Applicable to Esri Implementation and Training Services:** … not a service to be provided by Esri.
IT Security Certification & Accreditation Guidelines	20 pgs.	Describes the State of Maryland IT C&A process for Agency systems as a 4 phased activity – Definition, Verification, Validation and Post-Accreditation.	**Not Applicable to Esri Implementation and Training Services:** … not a service to be provided by Esri.
Firewall Policies	2 pgs.	Firewall Policies for Agency networks – Platform, Physical Security, Configuration, External Connections, Change Control, Logging and Enforcement.	**Not Applicable to Esri Implementation and Training Services:** … not a service to be provided by Esri.
Publicly Accessible Systems Policy	2 pgs.	Policies related to public-facing IT systems for State of Maryland agencies.	**Esri Complies** During implementation of any public-facing web services, Esri Implementation Services staff will comply with this policy.
Password Policy	3 pgs.	Policy for IT systems passwords for State of Maryland agencies.	**Esri Complies** It is anticipated that Esri staff will be provided with State of Maryland IT accounts. Esri staff will comply with DoIT password policies.
Remote Access Policy	2 pgs.	Policy for remote connections to DoIT systems for State of Maryland agencies.	**Esri Complies** It is anticipated that Esri staff may have remote connections to Maryland DoIT networks. Esri staff will comply with the DoIT remote access policy.

Wireless Communication Policy	2 pgs.	Policy for wireless communications to DoIT systems for State of Maryland agencies.	**Esri Complies** It is anticipated that Esri staff may have wireless connections to Maryland DoIT networks. Esri staff will comply with the DoIT wireless communications policy.
Acknowledge-ment of DoIT Electronic Communications Policy	1 pg.	Form for user of Agency's or State's electronic communications systems. Relevant to Esri employees on-site during the installation process.	**Esri Complies** It is anticipated that Esri staff will have access to Maryland DoIT systems and networks. Esri staff will complete the DoIT electronic communications policy acknowledgement form.
Email Encryption Policy	1 pg.	Relates to encryption of emails.	**Not Applicable to Esri Implementation and Training Services:** … Esri staff will not have State of Maryland email accounts.
Incident Report Form	1 pg.	PDF form for reporting IT security incidents to service.desk@maryland.gov	**Esri Complies** Esri staff will report IT security incidents using the Incident Report Form.