ADDENDUM TO
STATE OF MARYLAND PURCHASES
ISSUED UNDER
STATE MASTER CONTRACT NO. 060B6400028.

This addendum is applicable to each purchase order that is subject to the State of Maryland's contract number 060B6400028. 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. 060B6400028.

1. Section 18.19 Nonvisual Accessibility Warranty & Section 508 Compliance Policy. The Parties agree that section 18.19 Nonvisual Accessibility Warranty and 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."

2. 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.

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.

2.1. Section 18.17 – Security Requirements and Incident Response. With regard to the applicability of referenced DoIT policies in Section 18.17 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)).

2.2. Exhibit A and Exhibit C, section 3.4 Functional Area I - Desktop/Server Software (On-Premises Products).
To meet the requirements of Section 3.4 – Functional Area I - Desktop/Server 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](#).

2.1.3. Exhibit A and Exhibit C, section 3.4 Functional Area I - Desktop/Server Software (Cloud Product).

To meet the requirements of Section 3.4 – Functional Area I - Desktop/Server Software, Esri is offering ArcGIS Online as a component of Desktop licenses. 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.