Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

SERVICE AGREEMENT

between

The Maryland Department of Information Technology and

The Customer

for

Maryland Information Sharing and Analysis Center (MD-ISAC)

Cyber Threat Intelligence (CTI) Sharing and Collaboration Services

---

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

I. Service Description

The purpose of the Maryland Information Sharing and Analysis Center (MD-ISAC) is to produce timely, relevant, actionable cyber threat intelligence that meets the common needs across the breadth of state and local government stakeholders. Cyber-attacks present challenges for agencies and organizations that must defend their data and systems from capable threat actors. Given the risks that these threats present, it is increasingly important that agencies share cyber threat information and use it to improve their security posture.

MD-ISAC's Cyber Threat Intelligence (CTI) team analyzes cyber threat information from both open and closed sources to prepare it for sharing across customer organizations. Sharing methods include threat bulletins, email digest reports, as well as a self-service CTI portal. By exchanging CTI within a sharing community, agencies and member organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats an MD-ISAC member may face.

A. Standard Service:

The following components are included with the standard service:

- **Cyber Threat Bulletins & Email Flash Alerts**
  Compile and disseminate cyber threat data into cyber threat intelligence bulletins, reports, or alerts based on specific actors, attacks, campaigns,

or trends that either impact or have the potential to impact state agencies or local entities.

- **MD-ISAC Threat Intelligence Product (TIP) Member Org Environment & Access**
  MD-ISAC TIP Access (Anomali ThreatStream Member Edition) provides an online portal for the dissemination and sharing of threat bulletins, indicators of compromise (IOCs), and CTI submission by members.

- **Anomali Integrator**
  Anomali Integrator provides automated integration of MD-ISAC's CTI with the organization's existing security stack.

- **Cyber Intelligence Organization Alerts (Brand, Fraud, Credential Leaks, Dark Web, IP & Domain mentions)**
  Cyber Intelligence alerts help organizations further reduce external threats by receiving information about potential external risks to their brand vetted by MD-ISAC CTI analysts. Potential external risks may include, but are not limited to, typosquats, leaked data, domain abuse, dark web mentions, and organization (brand) impersonation.

- **Takedown services**
  Takedown services - In the event a domain abuse or organization (brand) impersonation with malicious intent has been confirmed, the MD-ISAC can initiate a takedown request to mitigate or reduce future risks.

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Incident Response (IR), Incident Handling (IH), and mitigation of identified threats, excluding the takedown services described above.
2. Vulnerability mitigation and management of related threats discovered or reported
3. Attack surface management
4. Forensic analysis
5. Malware analysis

C. Optional Services

Auxiliary services may be available upon request from the User Entity for an additional cost. These costs are not included in the budgeted services that DoIT provides and shall be the responsibility of the requesting agency or organization. For any work requested in this area, DoIT will not be able to proceed until fully funded by the requester through a separate statement of work (SOW) and funds certification document.

The following services are add-ons that may be requested. Costs for these items are variable and will be clearly defined and agreed to before moving forward with the request.

1. **Dark Web Market credential or data purchase validation** utilizing third-party **analyst-on-demand services**

II. Service Dependencies

To ensure the service described herein is delivered consistently and in accordance with state standards, the customer must meet the following requirements:

DoIT Services:	● No DoIT services or dependencies required
Technical:	● Organization designated email ● Web browser to access MD-ISAC Threat Intelligence Platform (TIP) ● MD-ISAC TIP member TIP account
Non-Technical:	● Points of contact (min 1 - max 5) for time-sensitive cyber threat bulletin dispensation, notable escalations, and coordinating organization changes or updates ● Identified TIP admin(s) responsible for creating and assigning member accounts ● Completed MD-ISAC onboarding form

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 30 calendar days from the posting date of the new service agreement.

A. DoIT Responsibilities for User Entity (Managed Agencies)
DoIT shall be responsible for the following activities in coordination with the User Entity receiving DoIT enterprise-managed services:

1. CTI Dissemination
   a) Threat Bulletins will be posted to the MD-ISAC platform and all relevant Agencies will be notified via automated email notification as soon as Threat Bulletins are posted. Agencies will be able to view Threat Bulletins from within the MD-ISAC platform.
   b) Threat Bulletins and IOCs will be posted to the MD-ISAC platform, and all organizations will be notified via automated email as they

are updated. Organizations will be able to view and export IOCs, from within the MD-ISAC TIP.

2. Manage CTI Platforms
    a) Threat Intelligence Platform (TIP) Infrastructure maintenance (maintained by Anomali)
    b) Threat Intelligence Platform (TIP) baseline configuration
    c) Coordinate TIP issues (Anomali is responsible for resolving technical issues)
    d) Anomali Integrator configuration*
    e) Anomali Integrator maintenance*
    f) Anomali Integrator downstream integration tuning/optimization
    g) Coordinate with TIP vendor (Anomali) for initial member org creation
    h) Maintain Recorded Future watchlist

    ***Anomali Integrator for members separate from DoIT instance will be managed by the organization, not DoIT**

3. Vendor engagement
    a) Support for issues and maintenance of SaaS applications

B. DoIT Responsibilities for User Entity (Non-Managed Agencies)

DoIT shall be responsible for the following activities in coordination with the User Entity for which DoIT does not provide enterprise-managed services:

1. CTI Dissemination
    a) Threat Bulletins will be posted to the MD-ISAC platform and all relevant Agencies will be notified via automated email notification as soon as Threat Bulletins are posted. Agencies will be able to view Threat Bulletins from within the MD-ISAC platform.
    b) Threat Bulletins and IOCs will be posted to the MD-ISAC platform, and all organizations will be notified via automated email as they are updated. Organizations will be able to view and export IOCs, from within the MD-ISAC TIP.
2. Manage CTI Platforms
    a) Threat Intelligence Platform (TIP) Infrastructure maintenance (maintained by Anomali)
    b) Threat Intelligence Platform (TIP) baseline configuration
    c) Coordinate TIP issues (Anomali is responsible for resolving technical issues)
    d) Anomali Integrator configuration*
    e) Anomali Integrator maintenance*
    f) Anomali Integrator downstream integration tuning/optimization
    g) Coordinate with TIP vendor (Anomali) for initial member org creation

***Anomali Integrator for members separate from DoIT instance will be managed by the organization, not DoIT**

3. Vendor engagement
   a) Support for issues and maintenance of SaaS applications

C. User Entity Responsibilities

The User Entity shall be responsible for the following activities:

1. Manages organization email distro account (if applicable)
2. Manages Org TIP accounts - coordinate, create, and maintain member access for other members within their organization
3. Proper handling of CTI received according to TLP guidelines
4. Submit cyber incidents through the Maryland Incident Report Form (when applicable)
5. (Optionally) submit CTI for sharing
6. Manage Anomali Integrator system configuration and maintenance (if applicable)

IV. Service Level Agreements (SLA's)

A. Availability

Service availability includes the duration of time the service is operational during a twenty-four (24) hour period and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	● MD-ISAC TIP member access: 99.9% uptime ● MD-ISAC / CTI staff hours: Monday through Friday, 0800-1800 EST, excluding holidays

B. Maintenance

DoIT may modify the service without degrading its functionality or security features.

1. Scheduled Maintenance

   Regular maintenance must be performed to maintain availability and reliability standards and includes replacing hardware, upgrading software, applying patches, and implementing bug fixes.
   a) Scheduled maintenance will be performed outside of normal business hours (8 pm - 6 am Monday - Friday; weekends and holidays) for non-SaaS applications
   b) The customer will be notified no less than five (5) business days prior to the scheduled activity for non-SaaS applications.

c) Within twenty-four (24) hours after the completion of the scheduled activity, the User Entity will be notified for non-SaaS applications.

2. Unplanned Maintenance
   a) DoIT will attempt to notify the User Entity of any unplanned maintenance activities no less than two (2) hours prior to commencement. Note: Emergency activities requiring immediate remediation may not allow ample time for notification.
   b) Within twenty-four (24) hours after the completion of unplanned maintenance activity, the User Entity will be notified.

C. Service Delivery

DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	Measure
Initial Ticket Response and Customer Contact	Within 24hrs - Monday through Friday
MD-ISAC TIP (SaaS) access	24x7x365
Member CTI Submission	Within 24hrs - Monday through Friday

V. Support and Service Management

A. Support

DoIT will provide support via telephone, email, or in-person according to the SLA's outlined above.

1. The DoIT Service Desk is available twenty-four (24) hours a day, seven (7) days a week, to provide Tier 1 telephone support.
2. Tier 2 support will be provided during regular business hours (8 am - 5 pm) Monday thru Friday, excluding state holidays and state closings.
3. Tier 3 support will be provided as needed to address further escalations
4. DoIT will serve as the primary support provider of the service outlined herein except when third-party vendors are employed.

B. Incident Management

Please contact the Security Operations Center (SOC) for all incident reporting at soc@maryland.gov (410-697-9700 Option #5)

C. Request Management

Requests to move, add, or change service shall be handled as follows:

1. Intake for New MD-ISAC Service(s) from DoIT

   Entities seeking to utilize the service or deploy optional services outlined herein must:

   a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
      - DoIT / MD-ISAC will evaluate the request to ensure that the service meets the entity's business needs.

2. Service Modifications

   To increase, decrease, or alter existing service, the User Entity must:

   a) Submit a request via email to md-isac@maryland.gov
      - Service modifications include increasing or decreasing quantity of units, duration of service, or changing subscriber tier.
      - DoIT / MD-ISAC will log the request and assign it to the appropriate team for fulfillment.
      - Requests involving increases in costs will result in billing changes to the agencies or organization, which will require a Statement of Work and fund certification to make the change.

D. Outages

DoIT will notify the User Entity via email of any outages or service degradation resulting from maintenance, fault isolation, or other disruptions.

E. Support and Service Management Exclusions:

While DoIT strives to tailor support and maintenance activities to match the customer's mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

1. Development or management of customer applications
2. Repairs or services for the customer's third-party technologies.
3. Spearheading User Entity initiatives
4. Project management

VI. Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale.

A. All services delivered by DoIT under this agreement will be supported via OSM appropriated funds unless identified consumption or specific requirements demand additional costs to support.

VII. Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

Due to the nature of the managed service and its alignment to the Statewide Cybersecurity Centralization Strategy, termination requires written authorization by the State Chief Information Security Officer (CISO). If approved, terminations will only be effective at the end of the fiscal year.

VIII. Warranty, Limitations, and Exclusions

A. N/A