Mandiant Statement of Work

Advanced Intelligence Analysis

Customer: Government of Israel – IAEC

This Statement of Work ("SOW") is part of the Purchase Order No. PO 5300003375 issued by the Government of Israel, Israel Atomic Energy Commission ("Customer") to Mandiant, Inc. including its subsidiary Mandiant Ireland Limited (referred to herein as "Mandiant"). This SOW is effective as of the last day of signature below ("SOW Effective Date"). This SOW is governed by the Terms and Conditions found at www.mandiant.com/company/legal ("Agreement").

Reference: Mandiant quote: Q-201324

1. DESCRIPTION OF SERVICES

For the Services Term (as defined below), Mandiant agrees to provide one (1) analyst for a defined period not to exceed two [2] days per work week (Sunday-Thursday), who is a Mandiant employee (the "AIA Integrator") to perform the following Services on-site at Customer's premises:

- Accessing and applying Mandiant's knowledgebase to improve and enhance the Customer's threat intelligence.
- Providing proprietary alert-driven threat reports describing Mandiant's knowledge of threat actors' identities, motives, capabilities, and targets.
- Preparing anticipatory analysis describing threat groups that are likely to target Customer, and the types of data theft or network attacks these groups would likely exploit;
- Collecting industry-specific analysis, such as case studies describing recent incidents at similar organizations, targeting trends across the industry, and new or expanded descriptions of threat actors specifically targeting the particular industry;
- Creating threat analysis reports describing new or evolving threats tied to the Customer's business areas, partners, products, and services;
- Deliver proprietary insights on the cyber threat landscape and specific threats facing Israel to improve situational awareness of current advanced persistent threat, financial, and criminal groups;
- Conducting digital threat assessments/monitoring on components, suppliers, and programs identified and prioritized by the Customer by using Mandiant's proprietary research tools to observe domain spoofing, dark web threats, and trending data from open sources and social media;

Promptly following the SOW Effective Date, Mandiant will begin the process of engaging the AIA Integrator. Customer acknowledges and agrees that Mandiant cannot guarantee the amount of time it will take to engage an appropriate AIA Integrator. Customer will have an opportunity to interview the AIA Integrator prior to engagement, and Customer may reasonably reject any candidate. The AIA Integrator will work from Customer's offices, be a citizen of the country in which the activities are to take place and will possess any necessary security clearances.

The Services described above are "Services" as defined in the Agreement.

The following are examples of the types of services that are not included in the Services described herein:

- Routine IT work such as troubleshooting and help desk functions
- Provision of bulk, raw intelligence from Mandiant's intelligence libraries
- Incident response activities
- SOC analyst work
- Penetration testing, vulnerability testing, or other proactive assessments

2. DELIVERABLES

Mandiant may provide the Customer with any or all the following items (each, "Mandiant Reports"), as requested through the AIA Integrator and as available:

- Alert-driven threat reports describing Mandiant's knowledge of threat actors' identities, motives, capabilities, and targets.
- Proprietary analysis describing threat groups that are likely to target Customer, and the types of data theft or network attacks these groups would likely exploit.
- Industry-specific analysis, such as case studies describing recent incidents at similar organizations, targeting trends across the industry, and new or expanded descriptions of threat actors specifically targeting the particular industry.
- Threat analysis reports describing new or evolving risks tied to the Customer's business areas, partners, products, and services.
- Digital threat assessments and dark web monitoring on components, suppliers, and programs identified and prioritized by the Customer;
- Threat landscape briefings providing situational awareness of current advanced persistent threat, financial, and hacktivists groups.

Mandiant Reports are "Deliverables" as defined in the Agreement. Subject to Customer's timely payment of applicable fees and expenses, and subject to this SOW, Customer shall have a perpetual, non-exclusive, nontransferable, right and license to use, display and reproduce the Mandiant Reports for its internal purposes only. Mandiant Reports may not be shared with or otherwise provided to any third party.

3. TERM

This SOW will become effective on the SOW Effective Date and continue for a term of two [2] days per work week for 12 months (52 weeks), on a Sunday through Thursday basis. (the "Term"). Each party may terminate this SOW as set forth in the Agreement.

4. FEES AND EXPENSES

In consideration of the Services and Deliverables described herein, Customer agrees to pay the fixed fees reflected in the Quote. Mandiant will invoice Customer the fees as set forth in the Quote on the SOW Effective Date.

5. ASSUMPTIONS

1. Fees do not include any hardware, software, licensing, maintenance or support costs of any Mandiant or other third-party product or service suggested by Mandiant as we conduct the activities outlined above.
2. Mandiant will provide Deliverables to Customer throughout this engagement. Draft deliverables are considered final upon confirmation from Customer (written or oral) or fifteen days after their submission date from Mandiant to Customer via email, whichever is earlier.
3. When Mandiant's personnel are performing Services on site at Customer's premises, Customer will allocate appropriate working space and physical access for all Mandiant assigned personnel.
4. Mandiant uses a (40) hour billable workweek as its standard, with approximately 30% of the AIA Integrator's time spent coordinating with Mandiant's Intelligence Team. On-site services for this engagement will be delivered over a two [2] day, (8) hours/day work period, on a Sunday through Thursday basis, unless otherwise mutually agreed. At Mandiant's sole discretion our analysts may elect to incur greater than 16 billable hours during this engagement.
5. Customer will make available key individuals within the appropriate cyber security program that can best help plan operations and activities.

6. CONTACT INFORMATION

Customer will provide contact information to Mandiant for those Customer personnel who are designated as Customer's points of contact for the Services.

Signature Page Follows

Mandiant Ireland Limited	**Government of Israel, Israel Atomic Energy Commission**
Signature	Signature
Name	Name
Title	Title
Date	Date