8840 Stanford Blvd # 2100
Columbia, MD 21045
(410) 290-1411
owlcyberdefense.com

Owl Cyber Defense Solutions, LLC
Supplier/Reseller Code of Conduct

Owl Cyber Defense Solutions, LLC (Owl Cyber Defense) is committed to promoting integrity, honesty, professionalism, and to maintaining the highest standards of ethical conduct in all of our activities and in the activities of those we do business with. As a result, Owl Cyber Defense has created this Supplier/Reseller Code of Conduct ("*Code*") for Owl Cyber Defense Suppliers (including Ow Cyber Defense consultants and contract labor), Owl Cyber Defense Resellers, and those who work for them, including employees, contractors, agents, consultants and subcontract labor to make sure that they too, promote integrity, honesty, professionalism, and the highest standards of ethical conduct (collectively referred to as "Supplier/Reseller").

Purpose of This *Code*

Prompt reporting of violations of this *Code* is required. Supplier/Resellers should report any concern that Owl Cyber Defense or any of its own executives or employees may have engaged in unlawful conduct or other violation of this *Code* to the Owl Cyber Defense Legal Department (jreed@owlcyberdefense.com), or by use of the Owl Cyber Defense Ethics Email (ethics@owlcyberdefense.com). Supplier/Resellers may report concerns openly and confidentially without fear of retaliation. However a failure to report such violation may result in an action taken against the Supplier/Reseller.

Compliance with Applicable Governmental Laws, Rules, and Regulations

Owl Cyber Defense requires any Supplier/Reseller that it does business with to comply with all laws, rules, and regulations applicable in any jurisdiction where the Supplier/Reseller conducts business. If a Supplier/Reseller has questions about whether particular circumstances may involve illegal conduct, or about specific laws that may apply to their activities, they should consult their own legal advisors.

Cooperation with Inquiries and Investigations

It is Owl Cyber Defense's policy to fully cooperate with any appropriate government investigation. If Owl Cyber Defense learns about a possible government investigation or inquiry that involves Supplier/Reseller, Owl Cyber Defense will notify Supplier/Reseller in accordance with any contracts/agreements with Supplier/Reseller.

Human Rights

Owl Cyber Defense requires Supplier/Reseller to comply with the relevant U.S. and international humanitarian laws with respect to human rights, illegal activity commonly referred to "trafficking in persons" or "human trafficking," as well as applicable customary laws and agreements. The U. S. Government and the Federal Acquisition Regulation detail a zero-tolerance policy regarding trafficking in persons to include: procuring sex acts; forced labor; and other actions which meet the definition of human trafficking. Specific examples of human trafficking may include: withholding employee passports; employment contracts and agreements not being written in the employee or subcontractor's native language; failure to provide a copy of the contract; failure to ensure that no employee pays a

recruiting fee to work; failure to provide adequate living conditions and failure to comply with the originating host country's transit, entry, and exit procedures. Owl Cyber Defense's commitment to human rights is further detailed in the *Owl Cyber Defense Anti-Trafficking Policy,* OWL-LG-PO-001.

Anti-Corruption and Bribery

Supplier/Reseller must comply with all anti-bribery and anti-corruption laws around the world. Supplier/Reseller is prohibited from offering, giving, soliciting, or accepting any bribe or kickback, whether dealing with government officials, political parties, or representatives of commercial organizations. Bribes include gifts, entertainment, travel, or other benefits of any kind. A kickback is providing or receiving something of value either to obtain or reward favorable treatment on a government contract or subcontract. There are serious consequences associated with a failure to disclose a potential bribe or kickback.

Supplier/Reseller must be committed to ensuring that all of its transactions and business dealings are conducted in compliance with the U.S. anti-corruption requirements. The U.S. Foreign Corrupt Practices Act ("FCPA"), the United Kingdom Bribery Act and the Anti-Kickback Act of 1986 (41 U.S.C. 51-58) are among the most stringent anti-corruption laws in the world and cover Owl Cyber Defense's Supplier/Reseller's international activities in many cases. The regulations prohibit government contractors and their Supplier/Reseller's, including their employees from soliciting or accepting anything of value from a downstream subcontractor, vendor, or supplier for the purpose of obtaining or rewarding favorable treatment.

It must be Supplier/Reseller's policy that their employees accept only business courtesies in circumstances that comply with both U.S. and host country law, and, further, that are reasonable in value, infrequently offered, and customary in a business setting. *Owl Cyber Defense's Global Anti-Corruption Policy*, OWL-LG-PO-003, further details Owl Cyber Defense's commitment to complying with the Anti-Kickback Act, Foreign Corrupt Practices Act, and the United Kingdom Bribery Act of 2010.

Business Courtesies and Gratuities

A business courtesy is a gift (anything of value) provided to a business counterparty, to include among other things meals, refreshments, entertainment, and admission to sporting events. In certain situations, the exchange of limited, non-cash business courtesies may be appropriate. Our Supplier/Reseller must not seek to improperly influence the decisions of Owl Cyber Defense's business counterparties or government officials by offering business courtesies, and Supplier/Reseller must require that the decisions of its executives and employees not be affected by having received a business courtesy. The Gifts, Travel, and Entertainment section of this *Code* addresses Owl Cyber Defense's policy on business courtesies, gifts, and gratuities with U.S. Government representatives that the Supplier/Reseller must abide by.

Supplier/Reseller must prohibit the solicitation, directly or indirectly, for its benefit or for the benefit of another person, of any gift, favor, or other gratuity or thing of value from a person or organization with which Supplier/Reseller does business or that seeks to do business with Supplier/Reseller. Soliciting a gift, favor, or other gratuity or thing of value is strictly prohibited regardless of the nature or value of the item or service.

Supplier/Reseller and its employees and business partners may not accept business courtesies that constitute, or could be reasonably perceived as constituting, unfair business inducements or that could violate law, regulation, or policies of Owl Cyber Defense or its customers or could reflect negatively on Owl Cyber Defense's reputation. Reference *Owl Cyber Defense's Global Anti-Corruption Policy* for additional details.

Supplier/Reseller executives and employees who have any questions about specific business courtesies, gifts or gratuities should obtain additional guidance in advance of the transaction from their legal advisors.

Gifts, Travel, and Entertainment

Gifts and Entertainment with U.S. Government Representatives

There are strict laws and regulations that govern the giving of gifts, gratuities, entertainment, and anything else of value to an employee of the U.S. Government. Examples include cash, gifts, meals, refreshments, transportation, and tickets to sporting or cultural events. It includes services as well as gifts of training, transportation, local travel, lodging, and meals, whether provided in-kind, by purchase of a ticket, payment in advance or reimbursement after the expense has been incurred. Supplier/Reseller is not permitted to give or offer anything of value to a U.S. Government employee except as permitted by law.

Gifts and Entertainment with Employees and Officials of Non-U.S. Governments

Under the Foreign Corrupt Practices Act ("FCPA"), the making of bribes, kickbacks, or other forms of corrupt, illegal, or improper payments to foreign government officials for the purpose of obtaining or retaining business is strictly prohibited. Foreign government officials include those employed by government agencies and bodies, as well as employees and executives of state-owned entities, such as hospitals, energy firms, and telecommunications providers. Prior to providing any gifts or if you have questions, Supplier/Reseller should consult their legal advisors.

Gifts and Entertainment with Non-Government Persons

Supplier/Reseller may provide meals, refreshments, or entertainment of reasonable value to non-government persons in support of business activities, provided:

- The business courtesy is not offered for favorable treatment;
- the courtesy does not violate any law, regulation, or standards of conduct of the recipient's organization. (It is your responsibility to inquire about any prohibitions or limitations applicable to the recipient's organization before offering any business courtesy.);
- The courtesy is consistent with marketplace practices, infrequent in nature, and is not lavish or extravagant.

Export, Customs, and Trade Controls

Supplier/Reseller must fully comply with all applicable export, customs, and trade control laws and regulations, licensing requirements, relevant countries', and international laws and applicable export and trade sanctions. Supplier/Reseller should consult with their legal advisors to answer any questions regarding customers, export licensing, and trade controls.

Conflicts of Interest

A personal conflict of interest occurs when an individual's private interest interferes in any way – or even appears to interfere – with the interests of Owl Cyber Defense or Supplier/Reseller. Generally, a conflict situation can arise when an employee or executive takes actions or has interests that may make it difficult to perform his or her duties and responsibilities objectively and effectively. Conflicts of interest also arise when you, or a member of your family, receive improper personal benefits as a result of your position with Supplier/Reseller.

Organizational Conflicts of Interest

Supplier/Reseller should always be aware of situations which may present an actual or potential Organizational Conflict of Interest (OCI) for Owl Cyber Defense or Supplier/Reseller, as defined in Federal Acquisition Regulation (FAR) Subpart 9.5, so that Owl Cyber Defense and Supplier/Reseller can take the appropriate steps to avoid or reduce the risk.

An OCI may arise when the work Supplier/Reseller performs on one contract creates an unfair advantage in competing for another contract, or when certain work or special access to a government program may impair or bias the contractor's ability to be objective and not conflicted in performing other work sought. OCIs fall generally into three categories:

- Unequal Access to Information. This usually arises when during contract performance, the contractor has access (not to include ordinary insight gained from incumbency) to nonpublic, proprietary, or source selection information not available to others and which provides an unfair competitive advantage.
- Impaired Objectivity. This usually arises when the contractor under the scope of one contract is required to evaluate work it, its affiliate, or its competitor performed on another contract.
- Ability to Set Biased Ground Rules. This usually arises when a contractor has the ability to set the ground rules (i.e., the specifications, scope of work, or requirements) for a solicitation that they, or their affiliate, can then pursue.

Where an actual or potential OCI may occur by entering into a contractual agreement or by accepting a task under an awarded contract, such contractual instruments may be entered into only after the following conditions have been satisfied:

- Supplier/Reseller must notify Owl Cyber Defense and affected parties of an actual or potential OCI, including conflicts between the interests of Owl Cyber Defense and/or Supplier/Reseller and the personal interests of a Supplier/Reseller's employees or those of close relatives, friends or business associates of a Supplier/Reseller or its employees.
- Cooperate as required to provide a full and complete disclosure of the actual or potential OCI to the appropriate governmental official(s) with a proposed means of avoiding, mitigating or neutralizing all perceived conflict(s), and,
- Consent to the execution of the contractual arrangement has been obtained from the appropriate governmental official(s), along with any necessary government approvals of an appropriate OCI avoidance and mitigation plan where required.

Supplier/Reseller must be aware of OCI certification clauses in government contracts and in all solicitations for which a bid is prepared. If Supplier/Reseller suspect that a situation may present an OCI risk, you must immediately report it to Owl Cyber Defense. OCI matters can be legally complex so you should always seek knowledgeable legal advice if you have any doubt. A failure to report such a situation may result in the termination for cause of the contract/agreement between the parties.

Procurement Integrity

In conducting business with government agencies, Supplier/Reseller is required to abide by certain special contract and procurement regulations and rules designed to protect the public interest the integrity of the government procurement processes. The Procurement Integrity Act provides a series of prohibitions designed to safeguard the integrity of the procurement process by ensuring that competitors for government contracts compete on a level playing field. Supplier/Reseller must not submit or concur in the submission of a proposal, price quotation, claim, or other document that is knowingly false, incomplete, or misleading. Supplier/Reseller is obligated to and must disclose, when required to do so, current, accurate, and complete cost and pricing data.

National Security

When supporting Owl Cyber Defense under a contract with the Department of Defense, Supplier/Reseller has a special obligation to comply with those government laws that protect our nation's security and safeguard our nation's secrets. The unauthorized possession of classified documents or classified information in any form or the failure to properly safeguard such information can endanger the security of our country and may be criminally or civilly punishable under espionage laws, among other applicable laws.

Disclosure Statements

Supplier/Reseller is committed to disclosure and transparency in accordance with FAR Clause 52.203-13 ("the rule"), 48 CFR §52.203-13 which requires Federal contractors to disclose in writing situations for which they have credible evidence of a potential violation of the civil False Claims Act or Federal criminal law involving fraud, conflict of interest, bribery, or gratuity.

Government Proprietary and Source Selection Information

Supplier/Reseller must not obtain, or seek to obtain, directly or indirectly, from any government employee or other third parties, any information believed to contain proprietary or source selection information, except where permitted by law or express agreement. Examples include: information contained in a competitor's bid or proposal, cost or pricing data, or other information submitted to the U.S. Government or contemplated for submission to the U.S. Government and designated as proprietary in accordance with the law or regulation.

Suspended and Debarred Contractors

Contractors that have committed certain specified offenses that indicate a lack of business integrity or responsibility may be suspended or debarred from doing business with the U.S. Government and many state and local governments. The names of the contractors suspended or debarred from federal

government contracting appear on the List of Parties Excluded from Federal Procurement and Non-procurement Programs ("excluded parties list").

Owl Cyber Defense will not do business with any Supplier/Reseller that has been suspended or debarred by federal, state, or local governments, nor will it contract with others to do business with any contractor or subcontractor that has been suspended or debarred by federal, state, or local governments.

Competitive Information

Collecting information on competitors from legitimate sources to evaluate the relative merits of their products, services, and marketing methods is proper and often necessary. However, the ways information should be acquired are limited. Supplier/Reseller are prohibited from using improper means in the gathering of competitive information. Any form of questionable intelligence gathering is strictly against Owl Cyber Defense policy.

The federal Procurement Integrity Act ("PIA") and trade secrets laws impose strict requirements on access to and use of protected, non-public information. Similar state and international laws govern fair competition. These laws prohibit the unauthorized disclosure and receipt of various types of "protected" or "off limits" information, including competitor bid and proposal information and U.S. Government source selection information. To ensure that procurements are free from favoritism or unlawful competitive advantage, certain information may not be released to, requested, or obtained, unless the information is released to all competitors or is made available publicly. Protected, or other non-public, information that is "off limits" includes:

- Competitor cost or pricing data, indirect costs, and direct labor rates;
- Customer source selection or technical evaluation plans;
- Customer technical or cost/price evaluations of proposals;
- Contractor bid and proposal information; and
- Competitor proprietary information about operations, technical solutions, or techniques.

Addressing Violations of this Code

Owl Cyber Defense must ensure prompt and consistent action in response to violations of this *Code*. Investigations of alleged violations of the *Code* will be conducted. If, after investigation, it is determined that Supplier/Reseller have violated the *Code*, the contract/agreement may be terminated for cause.