Policy #
Effective Date

HPC LLC

ITAR POLICY

V1

ADOPTED NOVEMBER 11, 2021

ELECTRONIC TRANSMISSION AND DATA STORAGE

Purpose

The purpose of this policy is to provide High Performance Conductors LLC employees required guidelines on electronic transmission procedures in accordance with U.S. Government laws and regulations (e.g., International Traffic in Arms Regulations (ITAR) 22 CFR 120-130, Freedom of Information Act, Electronic Communication Privacy Act of 1986, National Security Act, Storage Communication Act, and Executive Order 19528).

Supersedes

None

Roles Affected

This policy applies to all High Performance Conductors LLC (HPC) employees including the President, General Manager, Vice President, Executive Managers, Managers, and employees, as well as subsidiaries, contingent labor, and contract personnel.

References

Arms Export Control Act (AECA) 22 CFR USC 2778
Executive Order 19528
Freedom of Information Act (FOIA)
International Traffic in Arms Regulations (ITAR) 22 CFR Sections 120-130
Storage Communications Act (SCA)

A. Introduction

Electronic mail provides the ability to seamlessly transfer a massive amount of technical data across national and international borders with very little effort. Please be aware at all times that sending an e-mail may legally constitute an export, and consider the information being transmitted may be export sensitive. This policy will provide guidelines in

understanding the electronic transmission of Sensitive But Classified and/or Sensitive But Unclassified information.

B. Requirements

It is important that each HPC employee read and understand this policy. This will help minimize the risk to HPC and their employees. All HPC employees shall protect Sensitive But Classified and Sensitive But Unclassified information by the procedures contained in this policy.

C. Licensing Requirements for Technical Data

1. In accordance with ITAR 22 CFR Section 125.2 a license is required for export of any Unclassified technical data. Unless expressly exempted a license is required in the disclosure of technical data by U.S. persons to foreign persons regardless of the manner in which the technical data is transmitted (e.g., in person, by telephone, correspondence or electronic means). See Exemptions allowed in ITAR Section 125.4.

2. HPC employees exporting Classified technical data outside the U.S. must obtain approval by the Directorate of Defense Trade Controls (DDTC) for the export of technical data by a U.S. person to a Foreign person unless under exemption. See ITAR Section 125.3.

3. HPC employees are required to be aware of “deemed exports” an export of technology or source code (except encryption source code) is "deemed" to take place when it is released to a foreign national within the United States. See EAR Section 734.2.

D. Responsibilities

Company Commitment

1. Comply, maintain, and update this Company policy.

2. All HPC employees are responsible for complying with the requirements of software copyright licenses related to software packages used in fulfilling job requirements.

3. Classified material will be marked accordingly per Executive Order 12958.

4. Designated individual will provide access to sensitive information on a need to know basis.

5. Require establishment of security plans by all operators of computer systems that contain sensitive information.

6. Require HPC employees of the need to protect Company Classified and Unclassified information.

7. Will require a sensitivity determination be placed on all documents.

8. Enforce the procedures of this policy among HPC employees and within the workspaces for which they are responsible.

9. Require mandatory periodic training for all persons involved in management, use, or operation of a computer system that contains sensitive information.

10. Require HPC employees to read and understand this policy.

11. Provide access to an established procedure to investigate violations.

12. The Directorate of Defense Trade Controls (DDTC) will be informed and provide guidance on the investigation process of reported violations.

Managers

1. Ensures HPC will read, understand, and adhere to this policy, as well as U.S. laws and regulations concerning electronic transmission.

2. All managers are responsible for complying with the requirements of software copyright licenses related to software packages used in fulfilling job requirements.

3. Knowledge of when and how the Arms Export Control Act (AECA) 22 CFR USC 2778 and the International Traffic in Arms Regulations (ITAR) 22 CFR Sections 120-130 affect all Company controlled defense articles, defense services, and technical data.

4. Supervisors and managers shall ensure that only "authorized" employees have access to sensitive information through use of the HPC Server Access Form. See Attachment B.

5. Require establishment of security plans by all operators of computer systems that contain Sensitive But Classified and Sensitive But Unclassified information.

6. Will require employees of the need to protect Company information.

7. Require mandatory periodic training for all persons involved in management, use, or operation of a computer system that contains sensitive information. (e.g., use of appropriate Company log on and log off procedures, Disclaimer, and Company assets).

8. Will require a sensitivity determination be placed on all documents.

9. Enforce the procedures of this policy among HPC employees and within the workspaces for which they are responsible.

10. Address voluntary self-disclosures on potential violations of restrictions on export incidents.

11. Any person in possession of sensitive data is responsible for reporting the loss or possible inappropriate use of this information to Information Technology and Senior Management.

12. Provide access to an established procedure to investigate violations.

13. Report all violations of this policy of export authorizations, limitations, and restrictions associated with HPC LLC employees to the appropriate Senior Manager who will contact the DDTC.

Employees

1. All HPC LLC employees are responsible to read, understand, and comply with this policy.

2. Each HPC LLC employee is responsible for complying with the requirements of software copyright licenses related to software packages used in fulfilling job requirements.

3. Any person in possession of sensitive data is responsible for reporting the loss or possible inappropriate use of this information to Senior Management.

4. Provide voluntary self-disclosures on potential violations of restrictions on export incidents to appropriate internal authorities.

Compliance Department

1. Collaborates with Senior Management to ensure all HPC LLC employees have read, understood and comply with this policy.

2. Collaborates with Information Technology and Senior Management regarding loss of confidential data, and if the data in fact was licensable and export controlled.

3, All HPC LLC employees are responsible for complying with the requirements of software copyright licenses related to software packages used in fulfilling job requirements.

5. Provide voluntary self-disclosures on potential violations of restrictions on export incidents to appropriate internal authorities and contact the DDTC for further instruction.

6. Assist in Company audit procedures.

7. Ensure an internal audit program is in place to avoid potential violations.

E. Disciplinary Action and Enforcement

A violation of this Company policy may be cause for administrative action, including, but not limited to, removal from employment or discharge from HPC LLC. Violations of this policy may result in civil and criminal penalties, including fines and imprisonment, under the Federal or state laws of the United States.

Any suspected violation of Federal or state laws will be reported to the appropriate legal authority for investigation. Consequences for violations include, but are not limited to: Verbal warnings; revocation of access privileges; disciplinary actions up to and including termination of employment; and/or criminal prosecution. Potential or actual violations of this policy will be reported to the Directorate of Defense Trade Controls (DDTC) for investigation.

F. Potential System Abuses

1. Transmitting Top Secret, Secret, Confidential, Restricted or Classified, or Unclassified information without appropriate controls or appropriate authority.

2. Lack of electronic transmission Disclaimer. See appropriate electronic Disclaimer to be used:

"This message may contain HPC LLC Privileged/Proprietary information. If this email is not intended for you, and you are not responsible for the delivery of this email message to the addressee, do not keep, copy or deliver this email message to anyone. Please destroy this email in its entirety and notify the sender by reply email. Your cooperation is appreciated."

3. HPC LLC employees are accountable for inappropriate or illegal activity which would breach security or confidentiality relating to the use of electronic communication resources

4. Viewing or distributing sexually explicit, pornographic, racist, sexist, or material disparaging based on race, origin, sex, sexual orientation, age, disability, religion or political beliefs,

5. Viewing or sending messages intended to harass, intimidate, threaten, embarrass, humiliate or degrade another co-worker or that contain defamatory references.

6. Conducting illegal activity including gambling.

7. Using electronic communications resources for commercial uses not intended to benefit the Company.

8. Downloading or distributing pirated software or data, entertainment software, music or games.

9. Sending chain letters.

10. Propagating viruses, worms, Trojan horse, or trap door program codes.

11. Copying, destroying, deleting, distorting, removing, concealing, modifying or encrypting messages or files or other data on any company computer, network or other communications system without the permission of an authorized supervisor.

12. Conducting illegal activity including gambling.

13. Communicating in the name of the Company or contacting the media via a chat room or other electronic communications means.

14. Attempting to access or accessing another employee's computer, computer account, e-mail or voice mail messages, files or other data without their consent or the consent of an authorized supervisor.

15. Using resources for personal use that interferes with business operation, business productivity or distracts employees from their responsibilities.

G. Types of Sensitive Information

Sensitive But Classified and Sensitive But Unclassified information consist of any information exempted from the Freedom of Information Act (FOIA) and includes, but is not limited to, information related to personnel security, national security, and designated critical national electronic surveillance systems. Examples include, but are not limited to:

1. Sensitive But Classified is information includes information used in defense of national security of the U.S.; security information, including background investigation results and adjudication, and infraction/incident reports; personal information when associated with an individual's work on topics where security is involved or with those individuals who are authorized to have a level of access beyond the average employee, contractor, or visitor.

2. Sensitive But Unclassified is not a classification level for national security information, but is used when it's necessary to provide a degree of protection from unauthorized disclosure for unclassified information. SBU is used for two reasons: "... to keep classified material to a minimum and to be able to pass-on relevant, but sensitive information to individuals. Public access to "sensitive but unclassified" information would be limited to those with a

need to know and would be subject to provisions which govern disclosure and exemptions in the Freedom of Information Act and Privacy Act; unauthorized disclosure would be subject to penalties.

H. Information Protection

No HPC LLC may have any discussion or communication with any representative of a competitor concerning past, present or future goods or services to include pricing policies, bids, discounts, promotions, choice of suppliers, allocation of territories, sales or customers, limitations on production or distribution, or future location of stores. HPC LLC employees must not use their Company position to obtain improper personal benefit. No Company employee may use corporate property, information, or their position for personal gain.

HPC LLC has a duty to safeguard all confidential information of the Company or third parties which HPC LLC conducts business. The employee's obligation is to protect confidential information continues after he or she leaves the Company.

I. Marking Guidelines

Marking and labeling ensures communication of handling requirements. Markings on non- Lighted information should not be altered. See Executive Order 12958.

1. **Basic Methods:** When disclosed to Non-HPC LLC persons outside HPC LLC administrative control a Sensitive But Unclassified marking may be required to communicate a Proprietary interest in the information as follows:

   Technical Data Marking:
   EXPORT SENSITIVE BUT UNCLASSIFIED: ITAR CONTROLLED
   Information contained herein is subject to the Code of Federal Regulations Chapter 22 International Traffic in Arms Regulations (ITAR). This data may not be resold, diverted, transferred, transshipped, made available to a foreign national within the United States, or otherwise disposed of in any other country outside of its intended destination, either in original form

or after being incorporated through an intermediate process into other data without the prior written approval of the U.S. Department of State.

2. **Enhanced Controls:** Markings will be utilized when a marking is required to communicate Enhanced Controls HPC LLC ownership. Sensitive But Classified markings will include Technical Data, as well as Hardware, and may be required to communicate a Propriety interest as follows:

Technical Data:
EXPORT SENSITIVE BUT CLASSIFIED: ITAR CONTROLLED
Information contained herein is subject to the Code of Federal Regulations Chapter 22 International Traffic in Arms Regulations (ITAR). This data may not be resold, diverted, transferred, transshipped, made available to a foreign national within the United States, or otherwise disposed of in any other country outside of its intended destination, either in original form or after being incorporated through an intermediate process into other data without the prior written approval of the U.S. Department of State.

Hardware:
EXPORT SENSITIVE BUT CLASSIFIED: ITAR CONTROLLED
Hardware contained herein is subject to the Code of Federal Regulations Chapter 22 International Traffic in Arms Regulations (ITAR). This hardware may not be resold, diverted, transferred, transshipped, made available to a foreign national within the United States, or otherwise disposed of in any other country outside of its intended destination, either in original form or after being incorporated through an intermediate process into another product without the prior written approval of the U.S, Department of State.

Other additional markings may include HPC LLC Proprietary, when communicating specific sharing restrictions use the standard marking

and an additional control statement. For example:

HIGH PERFORMANCE CONDUCTORS LLC
Proprietary

HIGH PERFORMANCE CONDUCTORS LLC
Proprietary - Distribution Limited to ( )

J. Technical Data

Sensitive But Classified Technical information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. See ITAR Section 120.10. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation. This definition includes, but is not limited to, technical data belonging to HPC LLC customers and affiliates; information covered by an invention secrecy order; and classified information relating to defense articles and services. This also includes information that advance the state of the art of articles on the USML.

Sensitive But Unclassified information is that which has been generally available to the public in any form includes data released orally or visually at open conferences, lectures, trade shows, or other media open to the public include publications that may be purchased without restrictions at a nominal cost, or obtained without costs, or are readily available at libraries open to the public. See ITAR Section120.11.

Note: The Office of Defense Trade Controls has stated in public forum that a reasonable 'rule of thumb' which companies may use in helping evaluate whether or not information is technical data, for licensing purposes, is whether or not the company would readily provide the information to a competitor.

K. Technical Data Exemptions

Exemptions of general applicability apply to exports of technical data for which approval is not needed by the Directorate of Defense Trade Controls (DDTC) per ITAR Section 125.4. ITAR Section 125.5 includes Exemptions for Plant Visits. Certification Requirements for Exemptions are found in ITAR Section125.6.

L. Electronic Transmission

Electronic transmission includes messages, usually text, sent from one person to another via computer, fax, or other electronic device. E-mail and other electronic transmissions can also be sent automatically to a large number of addresses and may contain file attachments, images, and other forms of sensitive data.

Compliance personnel will be responsible for acquiring permission from the U.S. government to include licensing, necessary recordkeeping, and exemption addendums to allow electronic transmission of authorized technical data. A log of these exemptions and the e-mails they accompany will be kept on file.

Sensitive information should be encrypted and authenticated if it is sent from the Company network to an unsecured network. Sensitive information should never be communicated over wireless technologies, such as cellular or cordless telephones, or wireless data devices.

M. Faxing of Sensitive Information. Prior to faxing sensitive information, the sender should confirm that an authorized person will be present to accept the transmittal at the receiving end, or the sender should verify that the receiving facility is protected in a manner sufficient to preclude unauthorized access to the transmitted material.

N. Communicating Sensitive Information

1. From person to person in direct contact with one another.

2. Via telephone or video conference; (a license is required if communication of sensitive information is licensable controlled technology).

3. Via first class, priority, or overnight mail.

4. Via fax machine; (ensure a trusted source is available to receive fax).

5. Via e-mail to email that reside completely within the network that the sensitive data is encrypted and authenticated.

6. Sensitive information should not be transmitted via open network communication channels, including online video conferencing unless such a conference is held on a restricted network.

O. Release of Sensitive Information

1. Computer systems should be protected at all times by procedures established for information which has been specifically authorized under criteria established under Executive Order 12958 to be kept secret in the interest of national defense or foreign policy (e.g., protect information from being used to damage or endanger national security).

2. Different levels of protection based on the expected damage the information might cause in the wrong hands are contributing factors to the following levels of classifications (e.g., Top Secret, Secret, Confidential, Restricted, and Classified).

3. The primary purpose of standards and guideline shall be to control loss and unauthorized modification or disclosure of sensitive information.

4. Reasonable precautions should be taken to prevent access to sensitive information by persons who do not require the information to perform their jobs (e.g., sensitive documents should neither be read in a public place, nor taken home).

5. Sensitive information should only be released to authorized employees who have a specific job-related need-to-know for that information. The final responsibility for determining whether an individual has a need for access to sensitive information should be determined by the individual who has authorized possession, knowledge, or control of the information. Individuals responsible for sensitive information should be authorized to convey such information to others who have an official need-to-know.

P. Encryption Security

Encryption is a way to enhance the security of an electronic transmission by scrambling the contents so it can be read by someone who has the appropriate key to unscramble the message sent. Encryption has been found to be the most secure way in controlling sensitive information to be sent through electronic transmission.

Q. Information Risk Management

1. Control access to technical data based on user citizenship, certification training, computer system access and physical location.

2. Prevent leakage of technical data beyond certified systems and users.

3. Automatically match technical data export to licenses and/or TAAs.

4. Create information barriers around projects, applications and systems to prevent controlled technology to be released inadvertently.

5. Detect user activity that may constitute a Deemed Export and automate the processes of export licenses determination and manager approval.

R. Storage Rules for Sensitive Information

1. Sensitive information, both in hard copy and electronic form, should be physically protected and stored in limited areas.

2. Storing sensitive information in a property protection area or a public area is only acceptable if additional protections are taken to increase protection to a level comparable to that in a limited area.

3. All sensitive information existing in hard copy should be stored within a locked container in a limited or exclusion area, an access controlled electronic environment, or be under the physical control of an authorized individual.

4. Sensitive information should not be taken outside the United States.

5. Information handled electronically and transmitted over the network is at a higher risk of being released or altered.

6. Sensitive information stored on the network should be protected at a level that can ensure that only those who are authorized to view the information are allowed access (e.g., machine-generated passwords, encryption).

7. The network systems should maintain a high level of electronic protection (e.g., firewalls, intrusion detection, defense-in-depth, isolation of sensitive information, good practices network administration) to ensure the integrity of sensitive information and to prevent unauthorized access into these systems.

8. Regular review of the protection methods used and system auditing is also critical to maintain protection of these systems.

9. The physical elements of the network systems which store and transmit sensitive information or that have direct access to sensitive information should be secured appropriately.

10. The more central the information resource is (e.g., a network or security system control room) the higher the level of access control that should be applied.

S. Records Maintenance and Disposal

Controls are required to deter unauthorized access during disposal. Standard disposal methods include: See ITAR Section 122.5.

1. **Basic Methods:** Place information in the appropriate recycle locked container.

2. **Enhanced Controls:** Controls are required to prevent unauthorized access during disposal and to ensure that information cannot be reconstructed. HPC LLC can control disposal of their information by performing the following:

- Shredding the information
- Place information in a secured locked disposal bin
- Use a sanitation process to destroy all files (e.g., burning or disintegration).

Sensitive information should be destroyed by shredding or burning; paper containing sensitive information should not be recycled. Deleting, erasing, or formatting will not sufficiently remove sensitive information from electronic storage formats. Instead, files should be removed by using multiple passes (10 times minimum) of a hard drive wiping program.

Electronic or removable media should be physically damaged to the point of being inoperable, via shredding, degaussing, melting, or other such methods before disposal. In addition, it is important to state the disciplinary action that may be taken in the event of policy violation.

T. Corporate Audit

An audit may be required annually to determine if data integrity has been maintained. The IT audit is the process of collecting and evaluating

evidence to whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively, and use resources efficiently.

Data integrity relates to the accuracy and completeness of information as well as to its validity in accordance with the norms. An effective information system leads the organization to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. The IT Auditor must know the characteristics of users of the information system and the decision making environment in the auditor's organization while evaluating the effectiveness of any system per "Information Audit – General Principles."

U. Keep Accurate and Complete Records

We must maintain accurate and complete Company records. Transactions between the Company and outside individuals and organizations must be promptly and accurately entered in our recordkeeping system in accordance with generally accepted recordkeeping practices and principles. See ITAR Section 122.5(a).

V. Training

Public Law 100-235, the Computer Security Act of 1987, requires training for all employees responsible for the management and use of computer systems that process sensitive information. Under the regulation agencies will be responsible for identifying the employees to be trained and providing appropriate training.

Computer security basics are an introduction to the basic concepts behind computer security practices and the importance of the need to protect the information from vulnerabilities to known threats. Security planning and management is concerned with risk analysis, the determination of security requirements, security training, and internal agency organization to carry out the computer security function.

W. Obtain and Use Company Assets Wisely

Proper use of Company property, electronic communication systems, information resources, material, facilities, and equipment is the responsibility of each HPC LLC employee.

Use of these assets should be given the utmost care and respect, guarding against waste and abuse to include never borrowing or removing them from Company property without management's permission.

Personal use of Company assets must always be in accordance with corporate and Company policy. Consult your supervisor for appropriate guidance and permission. All HPC LLC employees are responsible for complying with the requirements of software copyright licenses related to software packages used in fulfilling job requirements.

EXHIBIIT A

DEFINITIONS

Arms Export Control Act

Act regulates the export of defense articles and services. Such exports may be licensed only if their export will strengthen United States national security, promotes foreign policy goals, or foster world peace. The Arms Export Control Act is administered by the Department of State, Center for Defense Trade Controls, through the ITAR and the United States Munitions List (defense articles that require a license prior to export).

Computer Security Act

"Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under section the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

Computer System

Computer System is defined as any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; and includes computers, ancillary equipment, software, firmware and similar procedures, services, support services; and related resources

Department of Commerce

The Department of Commerce is the United States federal department that promotes and administers domestic and foreign trade.

Department of State

The Department of State is the United States Federal department that sets and maintains foreign policies.

Export Administration Regulations (EAR)

Federal regulations implemented by the Department of Commerce that pertain to the export of commercial items not inherently military in nature (dual-use items). These regulations are contained in Title 15 of the Code of Federal Regulations (Sections 730-774) and include the Commerce Control List.

Electronic Communications Piracy Act

Title I of the ECPA protects wire, oral, and electronic communications while in transit. It sets down requirements for search warrants that are more stringent than in other settings. Title II of the ECPA, the Stored Communications Act (SCA) protects communication held in electronic storage, most notably messages stored on computers. Title III prohibits the use of devices to record dialing, routing, addressing, and signaling information used in the process of transmitting wire or electronic communications without a search warrant.

Electronic Transmission

Messages, usually text, sent from one person to another via computer, fax, or other electronic device. E-mail and other electronic transmissions can also be sent automatically to a large number of addresses and may contain file attachments, images, and other forms of sensitive data.

Encryption

Processing and altering data so only the intended recipient can read or use it. The recipient of the encrypted data must have the proper decryption key and program to decipher the data back to its original form.

Export
Sending or taking an article out of the U.S. in any manner. This includes, but is not limited to exports by mail, personal travel, courier service, e-mail, or network data transfers.

Export Controlled Information (or material)

Information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State. This pertains to items controlled by the ITAR, or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export Controlled Information must be controlled as "Sensitive But Unclassified" information and marked accordingly.

Freedom of Information Act

The Freedom of Information Act (FOIA) is the Federal law that provides access to federal agency records, except for certain types of records protected from disclosure under the Act. The law applies only to agency records in existence at the time of a FOIA request.

International Traffic in Arms Regulations (ITAR)

Federal regulations issued by the Department of State that regulate the export of items inherently military in nature. Items covered by the International Traffic in Arms Regulations (ITAR) 22 CFR Sections 120-130 are listed in Section 121 the "Munitions List,"

IT – Information Technology

Information technology refers to both the hardware and software that are used to store, retrieve, and manipulate information. At the lowest level you have the servers with an operating system. Installed on these servers are things like database and web serving software. The servers are connected to each other and to users via a network infrastructure. And the users accessing these servers have their own hardware, operating system, and software tools.

Non-Sensitive Data

Data that has been made generally available to the public in any form, including:

Data released orally or visually at open conferences, lectures, trade shows, or

other media open to the public; publications that may be purchased without restrictions at a nominal cost, or obtained without costs, or are readily available at libraries open to the public.

Privacy Act Protected Information

Information that if released could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals. Additional guidance may be found in the Privacy Act of 1974.

Proprietary Information

Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the Government's ability to obtain like information in the future, or impair the Government's interest in compliance with program effectiveness.

Sensitive But Classified

Classified information on aspects of security, including security plans, procedures, methods/measures, and equipment, for the physical protection of equipment, and facilities. Information is designated classified when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security, by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of defense articles, defense systems, or technical data.

Sensitive But Unclassified

This designation is applied to unclassified information that may be exempt from mandatory release to the public under FOIA. SBU is the formal designation for information that by law or regulation requires some form of protection but is outside the formal system of classification, as in accordance with Executive Order 12958.

Technical Data

Information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, and documentation. This definition includes but is not limited to technical data belonging to HPC LLC customers and affiliates.

EXHIBIT B

HPC LLC
SERVER ACCESS FORM

Requestor of access – Fill out form completely.

This form must be filled out for each requesting server access requested.

Send form to your Manager to approve and DIGITALLY SIGN by email – do not encrypt.

The manager will forward the completed form back to the Server Access group.

Requestor's Name:
Phone Number:
Approving HPC LLC Manager:

Access Level Requested:

☐ READ ONLY

☐ READ/WRITE

For the purpose of conforming to export compliance regulations. Record will be kept for 5 years.

ARE YOU AN HPC LLC EMPLOYEE? YES ☐ NO ☐

ARE YOU A U.S. CITIZEN? YES ☐ NO ☐