Exhibit A

#1924247

KOBAYASHI SUGITA & GODA, LLP
DAVID M. LOUIE 2162
JESSE W. SCHIEL 7995
First Hawaiian Center
999 Bishop Street, Suite 2600
Honolulu, Hawaii 96813
Telephone: (808) 535-5700
Facsimile: (808) 535-5799
E-mail: dml@ksglaw.com;
jws@ksglaw.com

Attorneys for Movant
PACMAR TECHNOLOGIES LLC f/k/a
MARTIN DEFENSE GROUP, LLC f/k/a
NAVATEK LLC

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. MARTIN KAO, Defendant.	CR. NO. 21-00061 LEK MOTION FOR RETURN OF PROPERTY PURSUANT TO RULE 41(g) OF THE FEDERAL RULES OF CRIMINAL PROCEDURE; MEMORANDUM IN SUPPORT OF MOTION; DECLARATION OF JAMES TOSHIZO OTA; DECLARATION OF JESSE W. SCHIEL; EXHIBITS 1 – 9; CERTIFICATE OF SERVICE

MOTION FOR RETURN OF PROPERTY PURSUANT TO RULE 41(G) OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

PACMAR TECHNOLOGIES LLC f/k/a MARTIN DEFENSE GROUP, LLC f/k/a NAVATEK LLC ("**PacMar**") files this motion pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure seeking the return of an Apple iPhone 11 Pro (IMEI 353247100759018, associated with the phone number ending in 0371), seized by the Department of Justice in 2020 at the time of Defendant MARTIN KAO'S arrest.

DATED: Honolulu, Hawaii, January 24, 2023.

/s/ Jesse W. Schiel
DAVID M. LOUIE
JESSE W. SCHIEL

Attorneys for Movant
PACMAR TECHNOLOGIES LLC
f/k/a MARTIN DEFENSE GROUP,
LLC f/k/a NAVATEK LLC

#1924247

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. MARTIN KAO, Defendant.	CR. NO. 21-00061 LEK MEMORANDUM IN SUPPORT OF MOTION

MEMORANDUM IN SUPPORT OF MOTION

I. INTRODUCTION

PACMAR TECHNOLOGIES LLC f/k/a MARTIN DEFENSE GROUP, LLC f/k/a NAVATEK LLC ("**PacMar**") seeks the return of Defendant MARTIN KAO'S ("**Defendant Kao**") Apple iPhone 11 Pro (IMEI 353247100759018) ("**Defendant Kao's Company Cellphone**"), used by Defendant Kao during his employment with PacMar, or in the alternative, the return of the call logs, voice message data, text messages, e-mails, and other forms of messaging; still and live photographs and video; audio files; storing dates, appointments, and other information on personal calendars, among other data (the "**Cellphone Data**") contained therein pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure.

PacMar retains a property interest in the return of Defendant Kao's Company Cellphone and the Cellphone data due to the nature of Defendant Kao's roles and

responsibilities during his employment with PacMar. Defendant Kao's Company Cellphone contains critical business and proprietary data belonging to PacMar that PacMar requires in its ongoing business operations.

PacMar has no other means to access this data other than by the return of Defendant Kao's Company Cellphone and the Cellphone Data by the United States Department of Justice (the "**DOJ**"), and such a return is not likely to affect or hinder the DOJ's investigation or prosecution of Defendant Kao for his criminal activities in the instant case.

II. STATEMENT OF FACTS

PacMar Technologies LLC was originally created in the 1970s under the name "Navatek Ltd." Since its formation, PacMar's focus has been on developing advanced ships to improve passenger ride quality, reduce operator injury, and improve hull efficiency. These engineering capabilities quickly led to innovations in hydrodynamic simulations, novel hull form designs, cutting edge motion control systems, and advanced marine prototype fabrication and testing. PacMar has since grown into a diversified technology company with a national presence, leading the way in research, engineering, design, and innovation.

Defendant Kao joined Navatek (now PacMar) in 2008, several decades after the Company had been formed and successfully operating. In or around August 2018, after forty successful years at the helm of the Company, Steven Loui,

PacMar's founder and then-President and CEO, decided to step away from the day-to-day management of the Company. He believed that he had found a worthy successor in Defendant Kao, who he believed would keep the Company prospering and would take care of its employees. Consequently, Mr. Loui relinquished his role as President and CEO to Defendant Kao, while retaining his role as Chairman and his ownership interest in the Company.

In 2008, and continuing through his tenure as President and CEO, Defendant Kao was issued a company cellphone to use for his role in PacMar's operations. Defendant Kao's receipt and use of a company cellphone was subject to PacMar's company cellphone policies. *See* Navatek Employee Handbook (Rev. 01/2010), at C-22 ¶ 6 ("If an employee is issued a company cell phone, this may not be used for personal phone calls unless authorized by the Company prior to usage. **All rules from this policy applies to company issued cell phones.**" (emphasis added)), attached as **Exhibit 1**; *see also id.* at C-23 § I ("Computers, computer files, electronic communication systems, internet access, and software furnished to employees are Company property intended to be used solely for business purposes. Any materials developed by an employee with company resources during or after normal work hours will be the property of the Company, including patentable inventions, copyrights, and trade secrets. **All work done with Company resources will be owned by the Company or will be deemed assigned to the Company**."

(emphasis added)); Declaration of James Toshizo Ota ("**Ota Decl.**") ¶ 7. The handbook further provides that "although incidental and occasional personal use of e-mail is permitted by the Company," the Company may access and disclose personal emails. *Id.* at C-23, § III. Defendant Kao acknowledged his receipt and understanding of these policies. *See* Acknowledgement of Employee Handbook, attached as **Exhibit 2**.

From 2018 on, as President and CEO of PacMar, Defendant Kao was responsible for oversight of all of PacMar's business operations, including review and supervision of the development of its products and technologies, communications with external parties in obtaining its contracts and subcontracts, review and oversight of internal processes and procedures related to its employees and management, and various other duties typical of a President and CEO of a federal contractor. PacMar continued to supply Defendant Kao with the use of a company-owned cellphone, subject to the same ongoing policies and conditions of use. *See* Martin Defense Group Information System Security Policies and Procedures Manual, at § 4.1(a) ("Martin Defense Group sensitive information stored on electronic and computing devices whether owned or leased by Martin Defense Group, a User, or a third party, remains the sole property of Martin Defense Group."), attached as **Exhibit 3**; MDG Employee Mobile Device Policy ("At any time upon request by Company management, the employee shall produce the mobile

device for return or inspection."), attached as **Exhibit 4**.

In 2020, around the time the DOJ arrested Defendant Kao, it seized various property, including certain Company property,[1] potentially relevant to Defendant Kao's crimes in the instant case. Among the items seized was an Apple iPhone 11 Pro (IMEI 353247100759018), associated with the phone number ending in 0371 ("**Defendant Kao's Company Cellphone**"). Defendant Kao's Company Cellphone was registered to a Company business account assigned to Defendant Kao, and was bought and paid for by Navatek LLC. (now PacMar) *See, e.g.*, Verizon Quick Bill Summary for Martin Kao, dated Jan. 12, 2020 (addressed to Navatek LLC and showing "Device Payment Agreement" charges of $1149.99 at page 2), attached hereto as **Exhibit 5**; Ota Decl ¶ 6.

By letter dated December 21, 2022, PacMar, by and through its undersigned counsel, requested that the DOJ return the Cellphone and/or the Cellphone Data, a true and correct copy of which is attached as **Exhibit 6**.

On December 29, 2022, Mr. Nolan, on behalf of the DOJ, responded by email correspondence to the undersigned and Mr. Victor Bakke, counsel for Defendant Kao, advising Mr. Bakke of the DOJ's intention to turn over the requested Cellphone Data to PacMar if no objection was made by 5:00 p.m. on Friday, January 6, 2023.

[1] The DOJ returned most of the Company assets seized, including the Company's servers, shortly after they were downloaded.

See E-mail from C. Nolan, dated Jan. 6, 2023, attached as **Exhibit 7**.

On Thursday, January 5, 2023, Mr. Bakke informed Mr. Nolan that Defendant Kao objected to the DOJ's release of the Cellphone or the Cellphone Data to PacMar, but did not explain on what basis the objection was made. *See* E-mail from V. Bakke, dated Jan. 5, 2023, attached as **Exhibit 8**.

By reply email on January 6, 2023, Mr. Nolan suggested to both counsel that the parties get the issue before the Court through a FRCP Rule 41(g) motion, and that the government would take no position (other than opposing any request to return the actual Cellphone). *See* E-mail from C. Nolan, dated Jan. 6, 2023, attached as **Exhibit 9**. For the avoidance of doubt, PacMar has no objection to the DOJ's return of the Cellphone Data in lieu of the return of the physical Cellphone.

III. APPLICABLE LEGAL STANDARDS

Rule 41(g) of the Federal Rules of Criminal Procedure provides that "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Fed. R. Crim. P. 41(g). "Though styled as a motion under a Federal Rule of Criminal Procedure, when the motion is made by a party against whom no criminal charges have been brought, such a motion is in fact a petition that the district court invoke its civil equitable jurisdiction." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1172 (9th Cir. 2010), *overruled on other grounds in Demaree v. Pederson*, 887 F.3d 870 (9th Cir.

2018) (per curiam). "That Rule 41(g) is broader than the exclusionary rule can no longer be in doubt in light of the 1989 amendments which explicitly authorize a motion to return property on behalf of any 'person aggrieved by an unlawful search and seizure of property or by the deprivation of property.' Fed. R. Crim. P. 41(g) (emphasis added). **This language was designed to expand the rule's coverage to include property lawfully seized.** *See id.* advisory committee notes." *Id.* at 1173 (emphasis added).

In considering a motion for return of property, the Court is required to balance four discretionary factors to determine whether to allow the government to retain the property, order it returned or (as happened in *Ramsden*) craft a compromise solution that seeks to accommodate the interests of all parties: (1) whether the movant is plainly aggrieved by the deprivation; (2) likely to suffer irreparable injury if it's not returned; (3) the lack of an adequate remedy at law; and (4) whether the government showed a callous disregard for the rights of third parties. *See id.* (citing *Ramsden v. United States*, 2 F.3d 322 (9th Cir. 1993)).

IV. ARGUMENT

A. PacMar is Plainly Aggrieved by the Deprivation of Its Property.

PacMar is plainly aggrieved by the seizure and failure of the DOJ to return Defendant Kao's Company Cellphone and the Cellphone Data contained therein. PacMar's business is the development of numerous, highly-specialized technologies

and concepts, and the Cellphone Data constitutes an otherwise irretrievable portion of that proprietary information. Similar to the movant in *Comprehensive Drug Testing*, PacMar has a plain property interest in the Cellphone Data. 621 F.3d at 1173–74 ("Here, the Players Association is aggrieved by the seizure as the removal of the specimens and documents breaches its negotiated agreement for confidentiality, violates its members' privacy interests and **interferes with the operation of its business**." (emphasis added)).

Further, due to Defendant Kao's role as President and CEO of PacMar from 2018 to 2020, Defendant Kao's Company Cellphone was used in the direct strategic planning and core operations of PacMar's business operations. Defendant Kao was *the* key decision maker in countless contract negotiations, strategic business decisions, internal communications, and oversight of the development of PacMar's products, which are typical of an individual who holds the position that Defendant Kao did during that time period. These strategic communications, business records, and other critical company information were not only critical to PacMar's operations through Defendant Kao's tenure as President and CEO, but continue to be necessary for PacMar's ongoing operations, as well as PacMar's ongoing handling of the consequences of Defendant Kao's criminal misconduct. As a federal contractor, PacMar is held to stringent standards in the course of its operations, and PacMar has

an ongoing duty to ensure that Defendant Kao's conduct has no lingering impact on PacMar's operations.

Thus, PacMar has a strong property interest in the return of the critical and proprietary data contained on Defendant Kao's Company Cellphone, which weighs in favor of the return of the seized property.

B. PacMar is Likely to Suffer Irreparable Injury if the Property is Not Returned.

As explained above, PacMar is seeking the return of Defendant Kao's Company Cellphone and the Cellphone Data not only for its importance in PacMar's ongoing business operations and strategic planning, but also to ensure that Defendant Kao's conduct has not and does not continue to affect PacMar's responsibilities and obligations as a federal contractor moving forward.

While PacMar typically retains access to company cellphones through software means, it has not had access to Defendant Kao's Company Cellphone or the Cellphone Data through any means since the seizure of the cellphone by the DOJ in 2020. *See* Ota Decl ¶ 8.

Because PacMar has no other means to access Defendant Kao's Company Cellphone or the Cellphone Data other than by its return to PacMar by the DOJ, and due to the critical and sensitive nature of the data and communications contained therein, the return of Defendant Kao's Company Cellphone and the Cellphone Data is necessary to ensure PacMar's continuing business operations and its compliance

with its obligations as a federal contractor. PacMar's ongoing business is likely to be jeopardized without a return of the seized property.

C. PacMar Has No Remedy at Law.

As explained by the Ninth Circuit in *Comprehensive Drug Testing*, since the 1989 amendments to the Federal Rules of Criminal Procedure, a motion made thereunder is the proper method of a third-party against whom no criminal charges have been brought. 621 F.3d at 1172-73. PacMar is not seeking to suppress any evidence obtained or intended to be used against Defendant Kao by the DOJ through this motion, and therefore has no other remedy at law for the return of Defendant Kao's Company Cellphone or the Cellphone Data.

D. The DOJ Has Not Shown a Callous Disregard for PacMar's Rights.

PacMar does not allege that the DOJ has shown a callous disregard for its rights in the seizure of Defendant Kao's Company Cellphone (or other PacMar property related to the criminal investigation which has since been returned to PacMar, *see* Statement of Facts, *supra* § II n.1). In fact, PacMar has provided assistance to the DOJ at numerous steps in its investigation of Defendant Kao's criminal activities, and continues to work with the DOJ to provide what assistance it can in the furtherance of justice. Further, it is PacMar's understanding that the

DOJ is not opposed to returning a copy of the Cellphone Data to PacMar.[2] *See* **Exhibit 7**.

V. CONCLUSION

For the foregoing reasons, as well as any further adduced at hearing of this motion, PacMar respectfully requests the Court issue an order directing the DOJ to return Defendant Kao's Company Cellphone to PacMar, or in the alternative, directing the DOJ to return a copy to PacMar of the Cellphone Data contained on Defendant Kao's Company Cellphone.

DATED: Honolulu, Hawaii, January 24, 2023.

/s/ Jesse W. Schiel
DAVID M. LOUIE
JESSE W. SCHIEL

Attorneys for Movant
PACMAR TECHNOLOGIES LLC
f/k/a MARTIN DEFENSE GROUP,
LLC f/k/a NAVATEK LLC

[2] PacMar also notes that Defendant Kao has pled guilty in the instant case, which further weighs in favor of the return of the seized property. *See United States v. Gladding*, 775 F.3d 1149, 1152 (9th Cir. 2014) ("'When a motion for return of property is made before an indictment is filed (but a criminal investigation is pending), the movant bears the burden of proving both that the [property's] seizure was illegal and that he or she is entitled to lawful possession of the property.' *United States v. Martinson*, 809 F.2d 1364, 1369 (9th Cir.1987) (citations omitted). **But that burden of proof changes when 'the property in question is no longer needed for evidentiary purposes, either because trial is complete, the defendant has pleaded guilty, or . . . the government has abandoned its investigation.**' *Id.*" (emphasis added)).

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. MARTIN KAO, Defendant.	CR. NO. 21-00061 LEK DECLARATION OF JAMES TOSHIZO OTA

DECLARATION OF JAMES TOSHIZO OTA

I, JAMES TOSHIZO OTA, declare and aver as follows:

1. I am over 18 years of age, am competent to make this declaration, and do so based upon personal knowledge, unless otherwise stated.

2. I was an employee of Navatek LLC during December of 2019, and my job title was Contracts Officer during this time. I am currently an employee of PacMar Technologies LLC (fka Martin Defense Group, LLC, fka Navatek LLC, hereinafter "**PacMar**"), and my job title is currently Contracts Officer and Comptroller.

3. I make this declaration in support of PacMar's Motion for Return of Property Pursuant to Rule 41(G) of The Federal Rules Of Criminal Procedure (the "**Motion**").

4. In my foregoing roles and as an employee of PacMar, I am knowledgeable and familiar with PacMar's employee policies, including PacMar's employee handbook and related company policies and procedures regarding the use of PacMar's property and equipment, including cellphones and related data.

5. Martin Kao was issued an Apple iPhone 11 Pro (IMEI 353247100759018) on or around January 2020 by PacMar for use in his duties and responsibilities as President and CEO of the company ("**Kao's Company Cellphone**").

6. Kao's Company Cellphone was bought and paid for by PacMar and was and remains the property of PacMar, including all data contained therein.

7. Mr. Kao's use of the Company Cellphone was, at all times, subject to PacMar's mobile device policies, which included that any and all data stored on company-issued cellphones, including e-mails, documents, or other electronic data, remained the property of PacMar.

8. PacMar has not been able to recover the data contained on Kao's Company Cellphone, which was seized by the Department of Justice in 2020 in connection with the underlying criminal case.

9. Attached to the Motion as **Exhibit 1** is a true and correct copy of the Navatek Employee Handbook (Rev. 01/2010), which was in effect between 2019-

2020 and remains in effect (the "**Handbook**"), and which Handbook PacMar maintains in its files in the ordinary course of business.

10. The Handbook contains PacMar's policies on business cellphones issued by PacMar to its employees, which has been in effect since January 2010.

11. Employees are required to sign an acknowledgement that they have read and understand the Handbook. That signed acknowledgement is maintained as part of each employee's personnel record.

12. Attached to the Motion as **Exhibit 2** is an Acknowledgment of the Handbook, signed by Martin Kao, which Acknowledgment PacMar maintains in its files in the ordinary course of business.

13. The Navatek Lifting Body Technologies LLC (Navatek LBT) Employee Handbook referenced in Mr. Kao's Exhibit 2 Acknowledgement is one and the same as the Exhibit 1 Handbook.

14. Attached to the Motion as **Exhibit 3** is a true and correct copy of PacMar's "Information System Security Policies and Procedures Manual" which was in effect between 2019-2020 and remains in effect, and which policy PacMar maintains in its files in the ordinary course of business.

15. Attached to the Motion as **Exhibit 4** is a true and correct copy of PacMar's "Employee Mobile Device Policy", which was in effect between 2019-

2020 and remains in effect, and which policy PacMar maintains in its files in the ordinary course of business.

16. Martin Kao was an employee of PacMar at all relevant times in 2019 and 2020 and was subject to the handbook and polices referenced in Exhibits 1, 3, and 4 above.

17. Attached to the Motion as **Exhibit 5** is a true and correct copy of a Verizon Quick Bill Summary for Kao's Company Cellphone, dated January 12, 2020, evidencing Kao's Company Cellphone expenses, including the expense of the phone itself, were billed to and paid for by PacMar.

I declare under penalty of law that the foregoing is true and correct.

DATED: Honolulu, Hawaii, 1/23/2023.

JAMES TOSHIZO OTA

#1925596

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. MARTIN KAO, Defendant.	CR. NO. 21-00061 LEK DECLARATION OF JESSE W. SCHIEL

DECLARATION OF JESSE W. SCHIEL

I, JESSE W. SCHIEL, declare and aver as follows:

1. I am an attorney with the firm Kobayashi Sugita & Goda, LLP ("**KSG**"), attorneys for Movant PACMAR TECHNOLOGIES LLC f/k/a MARTIN DEFENSE GROUP, LLC f/k/a NAVATEK LLC ("**PacMar**"). I am licensed to practice law before all of the state and federal courts in the State of Hawaii.

2. I am competent to testify as to the matters set forth herein and, unless otherwise indicated, make this declaration based upon my own personal information and knowledge.

3. I submit this declaration in support of PacMar's Motion for Return of Property Pursuant to Rule 41(G) Of The Federal Rules Of Criminal Procedure (the "**Motion**").

4. Attached to the Motion as **Exhibit 6** is a true and correct copy of a Letter sent from my office to Assisted United States Attorney Craig Nolan, requesting the return of Defendant Kao's Company Cellphone and/or the data contained therein, dated December 21, 2022. A copy of **Exhibit 6** is kept and maintained in KSG's files in the regular and ordinary course of business.

5. Attached to the Motion as **Exhibit 7** is a true and correct copy of an e-mail from AUSA Nolan to myself and Victor Bakke, notifying the parties of the DOJ's intent to keep possession of Defendant Kao's Company Cellphone, but to return a copy of the data to PacMar and inquiring as to whether Defendant Kao would object to this production, dated December 29, 2022. A copy of **Exhibit 7** is kept and maintained in KSG's files in the regular and ordinary course of business.

6. Attached to the Motion as **Exhibit 8** is a true and correct copy of Mr. Bakke's e-mail response, indicating that Defendant Kao would object to the production of Defendant Kao's Company Cellphone or any of the data contained therein, but not stating any formal bases for such objections, dated January 5, 2023. A copy of **Exhibit 8** is kept and maintained in KSG's files in the regular and ordinary course of business.

7. Attached to the Motion as **Exhibit 9** is a true and correct copy of an e-mail from AUSA Nolan inquiring as to a meeting of Defendant Kao and PacMar's respective counsel regarding the return of Defendant Kao's Company Cellphone

and/or the data contained therein and suggesting that PacMar should file a Motion under Fed. R. Crim. P. 41(g) to pursue a return of the cellphone and/or data. A copy of **Exhibit 9** is kept and maintained in KSG's files in the regular and ordinary course of business.

I declare under penalty of law that the foregoing is true and correct.

DATED: Honolulu, Hawaii, January 24, 2023.

/s/ Jesse W. Schiel
JESSE W. SCHIEL

Exhibit 1

Employee Handbook

For

Employees of

Navatek LLC

Navatek Alternative Energy Technologies, LLC.

Navatek CFD Technologies, LLC.

Navatek, Lifting Body Technologies, LLC.

Exhibit 1

TABLE OF CONTENTS

EMPLOYMENT PRACTICES

COMPENSATION

COMPANY REGULATIONS

EMPLOYEE BENEFITS

EMPLOYMENT PRACTICES

EMPLOYMENT STATUS

A **Full-time Regular** employee is defined as an individual employed by the Company on the following basis:

1. The individual is projected to work an average of thirty (30) hours or more per week.
2. The Employment Status Report reflects employment as being "Full-time Regular."
3. Full-time Regular employees are entitled to benefits as outlined, beginning on Page D-1 of this Handbook.

A **Part-time** employee is defined as an individual employed by the Company on the following basis:

1. The individual is projected to work an average of approximately twenty (20) hours or less per week.
2. The Employment Status Report reflects employment as being "Part-time."
3. Part-time employees are entitled to benefits as outlined, beginning on Page E-1 of this Handbook.

A **Full-time Temporary** employee is defined as an individual employed by the Company on the following basis:

1. The individual is projected to work an average of thirty (30) hours or more per week.
2. The Employment Status Report reflects employment as being "Full-time Temporary."
3. Full-time Temporary employees are entitled to benefits as outlined, beginning on Page D-25 of this Handbook.

EQUAL EMPLOYMENT OPPORTUNITY POLICY

The policy of Navatek, Ltd (the "Company") is to promote equal employment opportunity through a positive and continuous program of specific practices designed to ensure the full realization of equal employment opportunity, without regard to race, color, religion, sex, national origin, age, disability, ancestry, marital status, arrest and court record, sexual orientation, or status as a special disabled veteran or veteran designated under the Vietnam Era Veterans' Readjustment Assistance Act, as amended (VEVRAA). This reaffirms our commitment to this policy.

To implement this policy, the Company has, and will continue, to:

1. Recruit, hire, train and promote persons in all job classifications without regard to race, color, religion, sex, national origin, age, disability, ancestry, marital status, arrest and court record, sexual orientation, or status as a special disabled veteran, or veteran designated under VEVRAA.
2. Base decisions on employment so as to further the principle of equal employment opportunity.
3. Ensure that promotion decisions are in accord with principles of equal employment opportunity by imposing only valid requirements for promotional opportunities.
4. Ensure that all personnel actions (including but not limited to compensation, benefits, transfers, layoffs, return from layoff, Company sponsored training, education, tuition assistance, social and recreational programs) are administered without regard to race, color, religion, sex, national origin, age, disability, ancestry, marital status, arrest and court record, sexual orientation, status as a special disabled veteran, or veteran designated under VEVRAA.

Equal Employment Opportunity is a fundamental principle of our Company's operation. I expect each employee to cooperate to achieve this goal and I personally stand behind this principle.

BUSINESS ETHICS AND EMPLOYEE CONDUCT

Navatek, Ltd. maintains a reputation as a Company of the highest standards of lawfulness, responsibility and accountability. All employees shall at all times comply with all laws and the highest standards of business ethics and conduct wherever the Company conducts business; avoid situations which might involve a conflict between their personal interests and the interest of the Company, and those situations which create the appearance of conflict; and protect confidential and proprietary information held by the Company or entrusted to it. Employees must also avoid conduct on or off the job that may injure or harm the Company's reputation in the community, including but not limited to criminal conduct.

Compliance with this policy of business ethics and conduct is the responsibility of every Company employee. Disregarding or failing to comply with this policy could lead to disciplinary action, up to and including termination of employment.

PHYSICAL EXAMINATIONS / DRUG TESTING

All successful job applicants will receive an offer of employment conditioned on their completion of a physical examination to the Company's satisfaction at the Company's cost. All information gathered from medical examinations will be kept confidential by the Company and disclosed only to those persons who need to know the information.

During the course of employment with the Company, employees may be required at any time to undergo a physical examination(s) and/or drug testing, at a medical facility designated by the Company at the Company's cost. Time spent by an employee who undergoes a physical examination (s) and/or drug testing under this policy, will be considered compensable time worked, to a maximum of one (1) hour. (For more details on drug testing, refer to the Company's Substance Abuse Program in Section C)

JOB REFERENCES

It is the policy of the Company to restrict the release of information regarding its employees and former employees. Any persons or entities requesting information on a particular employee or former employee must direct their inquiries to the Corporate Human Resources Department. Upon request, only the following information will be provided on an employee or former employee:

- Verification as to whether the individual was or is employed by the Company.
- Verification of the individual's dates of employment.
- Verification of the individual's position.
- Verification of the individual's salary or rate of pay.

Exceptions to the above will be made for any employee or former employee who has displayed violence in the workplace.

Improper release of employee information may result in liability for both the Company and the employee releasing the information. Consequently, only designated Human Resources Personnel are authorized to disclose employee information. Current and former employees requesting job references must sign a written authorization for the release of employment related information. Company employees are prohibited from providing job references without written approval from the Corporate Human Resources Manager.

ATTENDANCE

Our Company depends on our employees to keep operations running smoothly. It is the responsibility of each employee to arrive at work on time, be ready to work at the scheduled starting time, and to keep absences to a minimum.

If you are unable to report to work due to illness, or for any other reason, you must notify your Supervisor as soon as feasible. Employees should also notify their Supervisor of the expected date and/or time he/she will report/return to work. Failure to notify your Supervisor of absences, tardiness or expected dates and/or times of return to work negatively impacts the Company's ability to perform to its customers' requirements and is therefore not acceptable. Furthermore, excessive absenteeism or tardiness is not acceptable, even though proper notices may have been given. Excessive absenteeism or tardiness may result in disciplinary action including termination from the Company. An employee who is absent for two consecutive work days without reporting or calling-in will be considered as having voluntarily resigned from employment.

APPEARANCE / WORK ATTIRE

Each of us is a representative of the Company. Therefore, it is the responsibility of each employee to represent the Company in a positive manner to its customers and the public through appropriate behavior and business attire. Employees are expected to be properly dressed and groomed.

Employees who report to work in unacceptable working attire, as listed below, may be sent home to change. Such time away from work will be unpaid.

Office and Administrative Employees:

Office and administrative employees must be dressed in casual business attire at all times during regular working hours. Clothing must be laundered, pressed and free of holes and tears. Proper undergarments and covered shoes or sandals must be worn at all times. A list of acceptable and unacceptable attire is provided below.

- Acceptable Attire:

  Men - long slacks or jeans, collared shirts, covered shoes, approved safety shoes or boots (safety toe or hard toe is acceptable) for those employees exposed to production operations, or sneakers

  Women - long slacks or jeans, dresses, skirts no shorter than 4 inches above the knee, shirts or blouses that fully cover the torso, covered shoes, sandals or sneakers

- Unacceptable Attire:

  T-shirts other than company t-shirts or tank tops; dresses, shorts or skirts shorter than 2 inches above the knee; any attire which reveals any part of the torso; exercise and workout attire including, but not limited to, running shorts, bicycle shorts and leotards and lycra crop tops; rubber slippers.

Production Employees:

- Acceptable Attire:

  Long slacks or jeans, collared shirts, uncollared T-shirts, coveralls, approved safety shoes or boots (safety toe or hard toe is acceptable)

- Unacceptable Attire:

  Shorts, no shirt, tank tops, sneakers, slippers or sandals or any other non-safety-type shoes

HONESTY

Honesty on or off-the-job, and our confidence in your trustworthiness and integrity, are absolute requirements. Dishonest acts are certain to be detected. The policy of the Company is to prosecute anyone, whether customer or employee, who misappropriates or steals money, merchandise, or property. It is your responsibility to report any dishonest acts to your supervisor immediately. Failure to do so may result in disciplinary action. You are also required to fully cooperate in any investigation of dishonesty, whether or not you are directly involved. Dishonesty or failure to fully cooperate in any company investigation of dishonesty is extremely serious misconduct which may result in disciplinary action, up to and including discharge.

PERSONNEL RECORDS

To comply with various government regulations, for benefit purposes and in case of emergencies, the Company maintains confidential personnel records on each employee. These records contain information such as name, address, telephone number, number of exemptions claimed on federal and state withholding taxes, marital status, number of dependents, beneficiary designations, and changes in work authorization. Failure to provide documentation of your identity and authorization to work, falsification of your application or verification documents and Form I-9 or expiration or revocation of work authorization is not acceptable and jeopordizes your employment.

It is important for your records to be current and accurate. It is the responsibility of each employee to keep his/her personnel record up-to-date by reporting in writing to his/her Supervisor, any changes or pertinent information that should be included in their personnel record.

The Company will disclose certain information concerning current or former employees in response to requests to verify employment for business reasons or to satisfy legitimate investigative or legal needs. Unless otherwise required by a subpoena or court order or a written release signed by the employee to release information, generally, information will be limited to verification of dates of employment, most recent position held, and salary data.

All personnel records, including an employee's personnel file, are the property of the company and are confidential. Employees who wish to view certain contents of their own personnel file should submit a written request to the Corporate Human Resources Manager for an appointment during normal working hours. You may inspect those documents which have been used to determine your qualifications for employment, promotion, additional compensation, termination, or other disciplinary action. You may not inspect information deemed confidential by the company. Review of your record will be with the Corporate Human Resources Manager or other designated Corporate Human Resources Representative. Copying or removal of personnel records by employees is not allowed.

RESOLVING PROBLEMS AND QUESTIONS

The Company believes it is important to handle employee problems and questions promptly and with fairness and justice. Problems, complaints and unanswered questions can affect your job performance and morale. It is important to treat those employees who present complaints with courtesy, dignity and consideration in discussing the matter.

Employees are encouraged to seek information or discuss their concerns with management. When misunderstandings or problems arise in connection with your work, you should discuss those misunderstandings or problems with your immediate supervisor. The Company believes that most matters will be satisfactorily resolved between the individual and the supervisor. To be sure that any questions or complaints you have is answered or resolved properly you should follow the chain of command as outlined:

1. First Step. Discussion with your immediate supervisor. If you were not satisfied with results of this discussion, you should write a statement then arrange a meeting with your Department or Division Manager.
2. Second Step. Discussion with your Department or Division Manager. If both of these discussions do not completely resolve the issue, you should call and arrange a meeting with the Corporate Human Resources manager.
3. Third Step. Discussion with Corporate Human Resources Manager. If this discussion still does not resolve the issue, you should call and arrange one final meeting with the Company President or General Manager.
4. Fourth Step. Discussion with Company President or General Manager. This is the final step in the Company's problem-resolution process.

Concerns or complaints involving any form of unlawful discrimination or harassment should be brought immediately to the Corporate Human Resources Manager. Such complaints will be investigated in accordance with the policy on Discrimination, Harassment and Sexual Harassment (Refer to Section C for the policy on Discrimination, Harassment and Sexual Harassment).

TERMINATIONS AND RESIGNATIONS

Your employment with the Company is at-will; that is, either you or the Company may terminate your employment at any time with or without notice or reason. Except in the case of termination for misconduct or poor performance, management will make an effort to notify employees in writing of their termination in advance.

If your employment is terminated by the Company, you will be paid your wages due in full at the time of discharge but not later than the next working day following your discharge. If you want to object to your termination, an appeal may be made to your Subsidiary/Division Manager or Corporate Human Resources Manager.

Employees who elect to resign from the Company at their discretion, are requested to give management at least two weeks written notice of their intent to resign so that a replacement may be found. Employees who quit or resign will be paid wages due in full not later than the next regular payday.

All employees who are leaving or who plan to leave their employment with the Company are asked to meet with a representative from the Corporate Human Resources Department prior to their departure for an exit interviewed. The purpose of the exit interview is to provide the employee with information regarding his/her separation from employment and to facilitate the return of the employee's company identification card(s), uniforms (if applicable), Employee Handbook, credit cards, keys, reports, company files, electronic files, or other items belonging to the Company in the employee's possession. The exit interview also provides the employee with an opportunity to express any opinions he/she may have regarding his/her employment with the Company. The employee will receive his/her final paycheck upon completion of the interview, return of all company property.

EVALUATION / ORIENTATION PERIOD

All new employees are required to undergo an evaluation / orientation period during the first ninety (90) working days of their employment with the Company unless otherwise noted. This period is intended to allow employees to become familiar with their responsibilities and company operations. Employees may be terminated at anytime and for any purpose for any reason with or without notice during this period as well as throughout their employment with the Company. The evaluation / orientation period may be extended as deemed necessary by the Supervisor, with the approval of management.

During this period, the new employee's performance will be subject to detailed evaluation by his/her Supervisor(s) to assist in the determination of the employee's retention or release.

PERFORMANCE REVIEWS

In addition to the day-to-day guidance you will receive from your Supervisor, your performance will be formally reviewed at the end of your orientation period and periodically thereafter. This review will give you and your Supervisor the opportunity to discuss your strong points, areas for improvement, and to set performance goals for the future.

TIMECARDS

An employee's timecards and/or timesheets are the official records of hours worked by an employee and are the basis for calculating payroll and maintaining accurate payroll records. Failure to complete one's timecard and/or timesheet correctly and on time may result in paycheck error and/or delay in issuing the employee their paycheck. Falsification, including incorrectly charging labor hours, of timecard and/or timesheet may be grounds for discipline including immediate discharge.

Each employee is responsible to correctly complete his/her own timecard and/or timesheet in its entirety. The employee is to record all hours worked corresponding to the job number. The employee must sign his/her timecard and/or timesheet and turn it in, on a daily or weekly basis, as specified by the Company, to his/her Supervisor for approval. Employees are not allowed to clock in or out, complete, or sign the timecard and/or timesheet of another employee. Employees who do so may be subject to discipline, including immediate discharge.

Any additions, corrections or other changes to be made on a timecard and/or timesheet after it is submitted must be reported to and approved by the employee's Supervisor. At that time, the employee will need to make necessary changes to the errors, initial and return it to his/her Supervisor for approval.

All employees will receive appropriate training in proper timekeeping procedures. Procedures for timecard and timesheet input are found in the employee file.

COMPENSATION

The Company compensates each employee based on his/her scope of responsibility, performance of job duties, and economic conditions, among other factors.

Employee performance is reviewed on an ongoing basis. Salary increases are based on performance as recommended by the employee's Supervisor and approved by management.

WORKWEEK & PAYDAYS

The normal workweek is from 12:01 a.m. on Sunday through 12:00 midnight on Saturday. The workweek generally consists of forty (40) hours per week.

Changes or modifications to your weekly or daily work schedule must be approved in advance by your Supervisor. Management reserves the right to change the work schedule for all employees due to unforeseen circumstances or as operational needs require.

Unless otherwise provided, paydays for salaried and hourly employees are bi-weekly on Fridays.

Should a holiday occur on pay day, paychecks will be issued the day prior.

As required by law, Federal and State Withholding tax and Social Security (FICA) tax deductions will be made from an employee's paycheck.

DIRECT DEPOSIT (ELECTRONIC FUND TRANSFERS – EFT)

Employees are given the option of having their paychecks electronically deposited in their bank accounts. In order to process a direct deposit request, an employee must complete a direct deposit form and attach a copy of a voided check and list the correct account number(s). The direct deposit form must be signed by the employee to give the Company the proper authorization to process the EFT.

After the employee initially enrolls in the direct deposit option, he/she may change his/her accounts and/or amounts designated for EFT a maximum of two (2) times per calendar year.

Processing time for direct deposit requests will vary depending on the specific financial institution. Generally the length of time is about 10 working days or a minimum of two payroll periods.

OVERTIME WORK

In order to meet operational needs, there are times when overtime may be required. An employee who works overtime and does not get hours authorized will be subject to discipline up to and including termination.

Overtime is calculated for hours worked in excess of forty (40) hours per week and will be compensated in either of two ways:

Wages. Full-time regular and full-time temporary employees paid on an hourly basis shall be paid at the rate of one and one-half (1-1/2) times his/her straight time hourly rate of pay for all hours worked in excess of 40 hours per week. Holiday hours and approved paid time off will be designated as credited hours within the work week.

Employees with fluctuating work schedules will be paid overtime in accordance with their individual written agreement.

Time Off. With their Supervisor's written approval, employees may schedule work times up to ten hours per day for four days and take the remaining hours during the week as time off.

The maximum time off that can be accrued at any point in time is forty (40) hours. All hours in excess of this amount will be paid in the normal course of payroll.

When overtime has been authorized and worked, the employee must complete and submit a timecard designating the overtime hours of work. Timecards for overtime must be turned in to the employee's immediate Supervisor for approval and processing no later than one (1) work day from the date the overtime was worked.

These overtime provisions shall not apply to employees that are considered "exempt" under State and Federal laws or regulations.

MILEAGE REIMBURSEMENT

Non-exempt employees who are directed to use their personal vehicles for business purposes will be reimbursed for mileage and parking fees. Mileage will be reimbursed at the current applicable Internal Revenue Code rate per mile. Use of one's personal vehicle for business purposes must be approved in advance by the President/General Manager and the Corporate Insurance Department.

Supporting receipts for parking fees and all mileage costs incurred as a result of business use must be submitted to the Company on the designated Mileage Reimbursement form. The Company may request additional information to substantiate any reimbursement request. Requests for mileage reimbursement must be submitted to the Accounting department with the necessary approvals no later than the 15th of the following month.

COMPANY REGULATIONS

STANDARDS OF CONDUCT

To maintain proper order within the Company and for the safety and protection of its employees and the visiting public, all employees are expected to adhere to certain standards of conduct in their relations with fellow employees, management staff and customers while on or about company premises and jobsites and/or company-sponsored functions inside and outside company premises.

The following is a list of prohibited employee conduct. It must be understood that this list merely provides examples of prohibited conduct and performance and is not intended to be a complete and exhaustive list of all offenses which may result in disciplinary action or discharge.

HOUSE RULES:

1. Insubordination, including improper conduct toward a supervisor or unwillingness, failure or refusal to perform work as required or assigned.
2. Use of profane or abusive language directed at a customer.
3. Physical aggression, fighting or attempting/threatening bodily injury to another employee, management staff or customer.
4. Any disorderly, immoral or indecent conduct including profanity directed at another employee, management staff or customer, etc. during working hours or on company premises.
5. Stealing, pilferage or willfully damaging property of the company, fellow employees, management staff and/or customers.
6. Improper or unauthorized use of company property, equipment, supplies and facilities for personal purposes.
7. Disclosing or disseminating confidential information without authorization.
8. Knowingly and intentionally disseminating or reporting false information about the company, management staff or fellow employees to any person, agency, or organization.
9. Falsification of timecard and/or timesheet, completing or signing timecard and/or timesheet for another employee or requesting another employee to complete or sign your timecard and/or timesheet or another employee's timecard and/or timesheet.
10. Falsification information provided for any company purposes including your employment application, applications for employee benefits, timecard, reports on status of job completions and accuracy of services, investigations of employee actions and activities, etc.

11. Release of employee information without authority and providing job references without written approval from the Corporate Human Resources Manager.
12. Sleeping on the job.
13. Failure to report accidents, injuries, breakage of or damage to equipment or falsifying or refusing to report incidents or to give testimony on incident investigations.
14. Permitting another employee to use key(s) without authorization for doors, closets, storage and other places under lock and key.
15. Neglect or disregard of posted smoking rules, safety rules, fire regulations, or sanitary rules and regulations.
16. Introduction, possession, or use on the job of drugs, narcotics or alcoholic beverages or reporting for work or attempting to work while under the influence of drugs, narcotics or alcoholic beverages.
17. Possession of firearms or weapons of any kind on company property.
18. Gambling of any form on company premises or during working hours.
19. Leaving the company premises or jobsite during working hours without authorization.
20. Loitering on company premises or jobsite during non-working hours.
22. Harassment, of any kind, directed toward Company employees, customers, visitors, or other persons at the worksite or while performing Company business away from the worksite.
23. Failure to comply with company policies, regulations, work rules, or directives not previously mentioned in the foregoing House Rules.

DISCIPLINE

The Company firmly believes that discipline serves to correct problems rather than punish employees. The basic means of helping employees correct their problems is the Company's system of progressive discipline.

Under the progressive discipline system, the Company will consider both (1) the nature and severity of the violation for which the employee is being disciplined and (2) the employee's disciplinary record when deciding on the disciplinary sanction the Company will impose. When the Company believes a sanction short of dismissal is sufficient to correct the conduct, the Company may impose a warning for a first violation or a warning and/or suspension from employment without pay for a second violation. Certain conduct, however, is so detrimental to the Company and its successful operation that immediate dismissal is warranted and prior warnings or suspensions are not appropriate. The company has the exclusive responsibility and authority to determine whether to discipline and when to discipline employees. The Company also reserves the right to determine the type and severity of discipline to be imposed in each case including, but not limited to, warnings, suspensions, and/or discharge.

The Company is dedicated to treating its employees fairly and impartially in imposing discipline. To ensure that any employee receiving discipline understands the disciplinary decision, his/her Supervisor may attempt when feasible, to discuss with the employee the reason for the sanction imposed and the consequences of future violations of any rules. Incidents of discipline will also be recorded in the employee's personnel file to be used in making decisions regarding promotions, demotions, discipline, discharge and other personnel matters.

SUBSTANCE ABUSE PROGRAM

I. PURPOSE

The Company recognizes that it is important to protect the health and safety of its employees, clients and the general public, and to improve the physical fitness and ability of its employees to perform their job. To assist us in achieving this goal, the Company has adopted the following substance abuse program (for drugs and alcohol) to achieve a drug-free workforce and workplace. The goals of this program are to educate employees about the problems of substance abuse and addiction, to assist employees in overcoming such problems, and to provide fair treatment of employees who are substance abusers. Accordingly, the Company has adopted the following.

II. POLICY

The unlawful manufacture, distribution, dispensing, possession or use of either alcohol or a controlled substance is prohibited on the Company's premises, its job sites and its property (vehicles, equipment, etc.) at all times. Furthermore, the Company prohibits employees from reporting to work or working under the influence of alcohol or drugs. Employees must notify their Manager if they take medications that have warning labels regarding the use of machinery, operation of vehicles, or which may cause drowsiness, nausea or similar side effects.

III. EDUCATION AND EMPLOYEE ASSISTANCE

A. Education. The Company has implemented and will maintain a substance abuse prevention program aimed at educating employees on the harmful effects of drugs and alcohol and stressing the provisions of this policy. In addition, supervisors will receive training to assist them in identifying and addressing substance abuse by employees.

B. Employee Assistance Program. The Company has established and will maintain an employee assistance program to help employees with substance abuse problems. For more information about the program, please contact the Corporate Human Resources Manager or the Employee Assistance Program Coordinator.

C. Self-Referrals. An employee with a substance abuse problem who desires to overcome such difficulty, and who voluntarily seeks help from management prior to being required to undergo drug testing will be referred to the Employee Assistance Program for help in overcoming the problem. An employee who voluntarily seeks and undergoes treatment, prior to being required to undergo drug testing, will not be subject to disciplinary action because of admitted substance

abuse. However, participation in the Employee Assistance Program will not shield an employee from disciplinary action should the employee violate the Substance Abuse Policy while undergoing treatment.

IV. DRUG TESTING

A. Drug screen testing will be required in the following situations:

1. For all applicants applying for employment.

2. For all employees returning from layoff or an unpaid leave of absence of one (1) month or more.

3. For all former employees who have not worked for the Company for a period of one (1) month or more at the time of rehire.

4. As part of the periodic physical examinations for all employees.

5. Where there is a reasonable cause to believe or reasonable suspicion to conclude that substance abuse is taking place. Examples of factors which may be considered include, but are not limited to: (a) excessive absenteeism; (b) frequent or unexplained absence from job site; (c) poor interpersonal relations on the job;
d) abnormal work performance or personal behavior; (e) exhibiting unsafe work habits or performance; (f) discovery of drugs or drug paraphernalia at the job site; (g) physical conditions or symptoms; and (h) objective evidence of illegal drug use or sale provided by any federal, state or local law enforcement agency.

6. When an employee is involved in an accident and/or is injured, as deemed necessary. However, employees falling within the following guidelines must be tested.

a. U.S. Department of Transportation Federal Highway Administration program guidelines. As soon as practicable, but not later than thirty-two (32) hours after an employee is involved in an accident or is injured. A driver who is seriously injured and cannot give a blood and/or urine specimen at the time of the accident, will provide the necessary authorization for obtaining hospital reports and other documents that would indicate whether there were any controlled substance(s) in his/her system.

b. U.S. Department of Transportation Coast Guard program guidelines. Upon the determination of a serious marine incident, all individuals engaged or employed on board the vessel who are directly involved in the incident will be tested.

7. Random Testing

b. Employees falling within the U.S. Department of Transportation Coast Guard program guidelines shall submit to random testing at an annual rate of not less than 50% for drug use. All crew members who must be tested are those (1) who occupy a position, or perform the duties and functions of a position, required by the vessel's Certificate of Inspection, (2) who perform the duties and functions of patrolmen or watchmen, or (3) who are specifically assigned the duties of warning, mustering, assembling, assisting, or controlling the movement of passengers during emergencies.

c. Employees falling within the U.S. Department of Transportation Federal Highway Administration program guidelines shall submit to random testing at an annual rate of not less than 50% for drug use and not less than 25% for alcohol use. Drivers who must be tested are those required to have a Commercial Driver's License (CDL) who drive a motor vehicle, (1) with a GVWR of 26,001 or more pounds inclusive of a towed unit with a GVWR of more than 10,000 pounds; or (2) with a GVWR of 26,001 pounds; or (3) designed to transport 16 or more passengers, including the driver, (4) of any size that is used to transport hazardous material which requires the vehicle to be placarded.

B. Applicants and employees required to undergo testing will be screened on a controlled and carefully monitored basis for marijuana and all THC containing substances, cocaine, amphetamines, PCP and opiates. Employees who are being tested for reasonable cause including involvement in an accident may also be tested for alcohol.

C. Blood and/or urine samples will be taken only under the direction of a licensed physician designated by the Company or under the direction of a designated medical laboratory facility. "Split Samples" will be taken to permit re-testing of the original sample.

Breath alcohol tests will be taken only by a breath alcohol technician trained to proficiency in the operation of the testing device in use.

D. Employees who are taking medication prescribed by a licensed medical practitioner should disclose this information to the Company and to the medical laboratory facility prior to them administering the test.

E. Time spent by an employee who undergoes a blood alcohol test or a drug screen test under this policy, will be considered compensable time worked, to a maximum of one (1) hour. However, this provision does not apply to job applicants or to "subsequent" tests while the employee is on suspension.

V. POSITIVE TEST READINGS

A. When an applicant's test reading is positive the applicant will be notified of the findings and will be rejected for employment.

B. When an employee's test reading is positive the employee will be notified of the findings, will be subject to disciplinary action in accordance with Section VI.A. below, and will be referred to the Company's Employee Assistance Program.

C. Department of Transportation Coast Guard program guidelines. If an employee holding a license, certificate of registry or merchant mariner's document has a positive test reading, the employee will be notified of the findings and the Company shall report the test results in writing to the Coast Guard Officer in Charge, Marine Inspection (OCMI). The employee shall be immediately removed from his/her duties which directly affect the safe operation of the vessel, will be subject to disciplinary action in accordance with Section VI.A. below, and will be referred to the Company's Employee Assistance Program.

D. An employee who tests positive and is later allowed to return to work pursuant to Sections VI.A.1. and 2. below will be subject to unannounced testing until two (2) subsequent consecutive tests are negative.

1. Such tests shall be conducted within twelve (12) months after the employee returns to work. The period for unannounced testing may be extended to comply with federal or state regulations.

2. Department of Defense and Department of Transportation (Coast Guard and Highway Administration). Such tests shall be conducted within sixty (60) months after the employee returns to work. The period for unannounced testing may be extended to comply with federal or state regulations.

E. Records on all positive test results will be retained for six (6) years and records on all negative results will be retained for twelve (12) months. These records are confidential and will not be disclosed unless required by law or authorized, in writing, by the employee tested.

F. An employee receiving a positive test result may, within sixty (60) days after receipt of the test result, submit a written request for re-testing of the specimen producing the positive test result. The sample may be provided to the original testing laboratory for re-testing. The laboratory will follow the established chain-of-custody procedures. The costs of the additional test, and all associated handling and shipping costs, will be the employee's responsibility. Written requests should be submitted to the Corporate Human Resources Manager and will be forwarded to the medical laboratory facility

VI. DISCIPLINARY POLICY

A. The following disciplinary action will be taken against an employee whose drug screen or blood alcohol test results in a positive reading:

1. First Offense. A suspension for the time it takes to obtain a negative reading from any subsequent test, but, in any case, no less than a two-week suspension and no more than a three (3) month suspension and referral to employee assistance program. The employee on suspension will determine when he/she wants to be subsequently re-tested. (The Company will pay for only one (1) retest.) However, should a subsequent test fail to produce a negative reading within three (3) months, the employee will be terminated.

2. Second Offense. A suspension for the time it takes to obtain a negative reading from any subsequent test, but, in any case, no less than a four-week suspension and no more than a two (2) month suspension and referral to the employee assistance program. The employee on suspension will determine when he/she wants to be subsequently re-tested. (The Company will pay for only one (1) retest.) However, should a subsequent test fail to produce a negative reading within two (2) months, the employee will be terminated.

3. Third Offense. Any employee who tests positive for the third time will be terminated.

B. The subsequent test as referenced in Section VI.A.1. and 2. above, taken after a positive reading to determine when an employee may return to work, will not be counted as an added offense.

C. Disciplinary action, up to and including termination, will also be taken under the following circumstances:

1. An employee refuses to sign a release and authorization to submit to any blood alcohol or drug screen test, or who refuses to undergo such a test, or refuses to permit the medical facility to provide the results to the company. Submission by an employee of an adulterated or diluted urine sample shall be construed as a refusal to test

2. An employee refuses to submit to a search of his personal property for contraband;

3. An employee refuses to submit to the Employee Assistance Program after being referred to the program by management;

4. Employees found in the possession of, using, consuming, selling or attempting to sell alcohol, illegal drugs and/or drug paraphernalia while on duty or on the Company's premises or job site;

5. An employee who fails to notify the Company within five (5) days of a conviction for drug violations which occurred when the employee was on duty or on the Company's premises or job site.

D. Employees who violate the Company's policy on substance abuse will be reported to the proper authorities for investigation and prosecution.

E. Department of Defense program guidelines. Employees convicted for drug violations which occurred while the employee was on duty or on the Company's premises or job site must notify the company no later than five (5) days after conviction. A company who is notified of an employee's conviction for a drug violation while the employee was on duty or on the Company's premises or job site must notify the Contracting or Granting Agency within ten (10) days after receiving actual notice that an employee has been convicted of a drug violation in the workplace.

VII. SEARCHES

A. The Company reserves the right, where there is a reasonable cause to

believe or reasonable suspicion to conclude that contraband may be present, to search employees' personal property including, but not limited to, lunch boxes, purses, bags, desks, lockers, or automobiles on the Company's premises or job sites without prior warning.

B. Any contraband or suspected contraband will be impounded and turned over to authorities for examination and/or analysis. A receipt will be issued for any seized property.

C. Time spent by an employee who undergoes a search under this policy, shall be considered compensable time worked.

VIII. DISCLOSURE OF INFORMATION

C. The records maintained by the Company for its Employee Assistance Program are confidential and protected by federal and state laws and regulations. The Company cannot disclose information identifying an employee as a participant in its program except in the following limited circumstances:

1. The employee-participant consents to the disclosure in writing
2. The disclosure is required by a court order;
3. The information is necessary to meet a medical emergency involving the employee-participant; or
4. The information is required by qualified personnel for research, audit or program evaluation.

B. The Company will provide each employee who participates in the Employee Assistance Program with a written summary, as requested, of the federal law and regulations governing disclosure as set forth in Exhibit B attached hereto and made a part hereof. The Company will request that the employee consent to release of treatment information to the Company by the treatment provider.

C. An employee's participation in the Employee Assistance Program will prohibit the Company and/or Employee Assistance Program provider from reporting any crimes committed by the employee-participant either at the program or against any person who works for the program, or from reporting any threats to commit such crimes, to the appropriate federal, state or local authorities.

D. An employee's participation in the Employee Assistance Program will not prohibit the Company and/or Employee Assistance Program plan provider from reporting any information about suspected child abuse or neglect under state law to the appropriate state or local authorities.

DISCRIMINATION, HARASSMENT AND SEXUAL HARASSMENT

Navatek, Ltd. is firmly committed to a policy of non-discrimination and the right of all employees to a work environment free of harassment and intimidation. Discrimination or harassment of any employee on the basis of age, sex, religion, race, color, national origin, disability, marital status, sexual orientation or arrest and court record, pregnancy, and genetic information is prohibited. Furthermore, unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature by any employee to any other employee are serious violations of the Company's policy against sexual harassment and will not be tolerated.

Unwelcome verbal, non-verbal, visual, or physical conduct of a sexual nature constitute inappropriate sexual conduct, which can form the basis of sexual harassment claims. Inappropriate sexual conduct can take many forms. It is not limited to physical assaults, unwelcome or unwanted sexual advances, or requests and demands for sexual favors. It can also involve:

- Unnecessary or unwanted physical contact (e.g. patting, pinching, hugging or intentional brushing up against another's body);

- Verbal conduct (e.g. offensive sexual flirtations, advances, propositions, verbal abuse of a sexual nature, graphic verbal commentaries about an individual's body, sexually degrading words used to describe an individual or the telling of "dirty jokes"); and

- Non-verbal conduct (e.g. the display in the work place of sexually suggestive objects or posters and calendars showing nude or partially nude photographs, winking, lingering glances, wolf whistles, sexual gestures).

Inappropriate sexual conduct becomes unlawful sexual harassment when: (1) submission to such conduct is made a term or condition of an individual's employment; (2) submission to or rejection of such conduct is used as a basis for employment decisions affecting the individual; or (3) such conduct has the purpose or effect of interfering with an individual's work performance or creates an intimidating, hostile or offensive working environment.

All employees are responsible for compliance with this policy. Where management determines that sexual or other harassment may have occurred, it will take immediate and appropriate corrective action to end the harassment, make the victim whole by restoring lost employment benefits or opportunities, if applicable, and prevent the misconduct from recurring.

Any employee who feels he or she has been subject to discrimination, harassment or sexual harassment, should contact either their supervisor, department head, manager or the Corporate Human Resources Manager/EEO Officer, immediately. An investigation into the surrounding circumstances will be conducted, keeping it confidential to the extent possible, to resolve the matter promptly. Retaliation in any form against an individual who has filed a complaint of discrimination or harassment will not be tolerated.

VIOLENCE PREVENTION

I. POLICY

The Company has a zero tolerance for violence. Any employee who displays any violence in the workplace or threatens violence in the workplace, will be subject to immediate termination from employment. No talk of violence or joking about violence will be tolerated.

"Violence" is defined to include physically harming another, shoving, pushing, harassment, verbal or physical intimidation, coercion, brandishing weapons, and threats or talk of violence.

II. SAFE WORKPLACE COMMITMENT

We are committed to providing a safe environment for employees, customers, vendors and visitors. In order to provide a safe workplace, the following rules apply:

A. Property Access. Access to our property is limited to those with a legitimate business interest. All employees and employee vehicles entering the property must display a valid company parking sticker. All visitors and visitor vehicles must register and display a Visitor Parking Pass while on company property.

B. Inspections. Desks, telephones and computers are company property. The Company has the right to enter or inspect work area including, but not limited to, desks, lockers, computers and computer storage disks, with or without notice.

C. Equipment. Our fax machines, copiers and mail systems, including E-mail, where applicable, are for business purposes. Personal business should not be conducted through these business systems. Under conditions approved by the management, telephone conversations may be overheard and voice mail messages may be retrieved in the process of monitoring customer service.

D. Threats. Any private conversations overheard or private messages retrieved during such monitoring constituting threats against other individuals will be a basis of termination from employment.

IV. CORRECTIVE ACTION

To ensure consistent treatment of all our employees, we have a corrective action system. Should there be a problem regarding your adherence to our policies and work rules, you may be given an opportunity to change the inappropriate behavior.

V. EMPLOYEE ASSISTANCE PROGRAM

We provide the resources of an employee assistance program (EAP) to all of our full-time employees. (See Section D for more details on EAP services.) EAP services are offered to these employees and their eligible dependents. While we receive periodic reports on the number and types of visits made to the EAP, we do not receive any information about individual contacts, or matters discussed during scheduled sessions.

You are encouraged to use our EAP whenever you feel the need for guidance in coping with any problems you have. If you have difficulty with the use of drugs or alcohol, the EAP can provide information on treatment.

The EAP is a confidential service to be used when you need help.

VI. REPORTING POTENTIAL PROBLEMS

It is everyone's business to prevent violence in the workplace. You can help by reporting what you see in the workplace that could indicate that a co-worker is in trouble. Often, you are in a better position than management to know what is happening to those you work with.

You are encouraged to report any incident that may involve a violation of our policies that are designed to provide a comfortable and safe working environment. Concerns may be presented to your supervisor, manager or the Corporate Human Resources Manager.

All reports will be investigated promptly and information will be kept confidential, except where there is a need to know in order to resolve the problem. The Company prohibits retaliation against any employee who has made a good-faith complaint of intimidation, harassment, or threat of violence or who has cooperated with the investigation of such a complaint.

VII. WORKPLACE INCIDENTS

In the event of a major workplace incident that affects or has the potential to affect the mental health of our work force, we may provide initial counseling and support services to you and your immediate family members.

As the crisis passes and support systems are put into place for individuals affected by the incident, we will make every effort to return to normal business operations. A reasonable effort will be made to notify employees, customers and others who need to know of the status of our business operations directly whenever possible. In cases where direct contact is not possible or practical, an effort will be made to communicate through the news media and other available resources.

SMOKING POLICY

I. PURPOSE AND BACKGROUND

A. This policy is designed to promote employee health and safety and the conduct of company business. It is not intended to totally prohibit smoking on the Company's premises, but does restrict it to certain areas.

B. Smoking poses a significant risk to a smoker's and non-smoker's health. It can also damage sensitive technical equipment and can be a safety hazard. In sufficient concentrations, side stream of second-hand smoke can be annoying to non-smokers. It may be harmful to individuals with heart and respiratory diseases or allergies related to tobacco smoke.

C. Smoking is a complex problem that concerns elements of a psychological and physiological addiction. Many individuals require assistance to eliminate smoking from their lives. It is not a problem that can be solved completely by prohibition or restriction. This policy is intended to assist employees in finding a reasonable accommodation between those who do not smoke and those who do, and demonstrates the Company's desire to encourage good health for all employees.

D. According to the Hawaii Smoke Free Law, the Act is to protect the public health and welfare by prohibiting smoking in public places and places of employment to ensure a consistent level of basic protections statewide from exposure to secondhand smoke.

II. POLICY

It is the Company's policy to respect the non-smoker's and the smoker's rights in company buildings and facilities. When these rights conflict, the Company and its employees should endeavor to find a reasonable accommodation. When an accommodation is not possible, the non-smoker's rights should prevail.

III. PROHIBITED AREAS

Smoking is not permitted:

A. In all enclosed or partially enclosed areas, including buildings and vehicles owned, leased, or operated by the State or any county.

B. In all enclosed or partially enclosed areas of places of employment, which includes a minimum distance of 20 (twenty) feet from entrances, exits, windows that open, and ventilation intakes that serve an enclosed or partially enclosed area where smoking is prohibited.

C. In areas with sensitive equipment, computer systems, or where records and supplies would be exposed to hazard from fires, ashes or smoke;

D. Where combustible fumes can collect, as in garage and storage areas, areas where chemicals are used, and all other designated areas where an occupational safety or health hazard might exist;

E. In confined areas of general access, as in restrooms, copy rooms, the conference room, etc.;

F. Aboard all vessels.

G. Where company premises are frequently visited by customers, such as public offices and customer service areas; and

H. The Company may designate locations where smoking specifically is permitted.

CONFLICT OF INTEREST

A successful working relationship with the Company requires your full effort and attention. Outside interests should be avoided if they might adversely affect your employment with the Company including conflict with the Company's interests. Examples of conflicts of interest include, but are not limited to:

* Outside activities including part-time employment, which have a negative effect on your ability to satisfy job-related requirements of your position with the Company;
* Outside employment or business interests, which are in competition with the Company's business; and
* Outside activities, which involve the use of confidential information learned directly or indirectly through employment at the Company.

You are required to report all outside employment and business interests to your Department or Division Manager in order to determine if there is any possibility of a conflict of interest. You are also requested to report any other activities that might be regarded as a conflict of interest. Failure to report potential conflicts of interest or refusal to resolve such conflicts may result in disciplinary action, including discharge.

SAFETY AND HEALTH

The safety and health policy for the Company provides the basis for the safety and health program. Accident prevention is a management function and responsibility. However, all employees should work toward a goal of zero accidents, injuries/illnesses. We will provide a safe and healthful work place through the identification of hazards and mitigation of them to prevent injuries and illnesses. Employee involvement in the identification and mitigation of hazards is an integral element to our success. The involvement of employees in every aspect of our safety and health program also includes a policy that employees are protected from any discriminatory or reprisal actions as a result of their participation or involvement.

Implementation of the safety and health program is the responsibility of the first line supervisors. Managers are responsible for ensuring that the safety and health programs are developed. Meeting their responsibilities in providing a safe and healthful work place requires knowledge of the company safety and health program, application of the program elements to the daily work activities, monitoring the implementation methods and correcting deficiencies or unsatisfactory trends.

Employees are expected to participate in the implementation of the safety and health program through suggestions for improvements, identification of hazards or potential hazards, and compliance with the program requirements, e.g., wearing of personal protective equipment, participating in work place monitoring activities to determine employee exposure, reporting accidents, injuries, or illnesses, and complying with procedures and safety related signs, tags, and barricades.

Protection of our employees and the environment are top priorities and must be considered in all decisions regarding our work operations. Implementing and integrating the safety and health regulations, Federal and State, with our work activities are expected to further our efforts to eliminate accidents, injuries and illnesses.

CONFIDENTIALITY

It is the Company's policy to protect its property and sensitive information. The willful disclosure of confidential Company information constitutes violation of Company policy and may result in disciplinary action up to and including discharge for current employees and legal action against former employees. The information not to be released to people and entities outside the Company includes, but is not limited to, the following:

* Marketing goals and/or margins
* Sales Figures
* Customer spending, lists and other data
* Profit margins
* Product Mark-up
* All Company reports such as sales reports, operating reports
* Photocopies
* Names and addresses of employees or customers
* Employee handbook
* Employee compensation
* Project documents, records, studies, internal memos, grant proposals
* Contracts and supporting documentation
* Communications (emails, letters, other social media venues) to and from customers, partners, government agencies, independent contractors and others who deal with company business
* Computer files and data
* Proprietary processes, trade secrets, and intellectual property of the company, or owned by clients/customers and shared with the company.

These company related materials should not be shared with people outside the company. If you are unsure of the materials' confidentiality, please check with your supervisor.

COMMUNICABLE AND LIFE-THREATENING ILLNESSES

The Company is committed to providing a healthy work environment and to protecting the physical and emotional health and well-being of all employees in the workplace.

We recognize that employees with communicable or life-threatening illnesses, including but not limited to cancer, heart disease, AIDS, hepatitis and tuberculosis, may wish to continue working for as long as their condition allows, providing the employee's condition does not pose a threat to the health of other employees.

As with any illness or disability, employees are permitted to continue to work as long as acceptable performance standards are met and medical evidence indicates that their illness is not a threat to others. Such persons will be treated consistently with other employees.

Any employee diagnosed with a communicable or life-threatening illness is entitled, as is any other employee, to confidentiality of information regarding their medical condition and records. All precautions to protect such information will be taken.

No other accommodation will be provided as long as medical advice indicates the work environment is a safe one. Education will be provided to members of such a work group as necessary.

CELLULAR PHONES

Purpose

The purpose of this policy is to promote a safe and productive work environment and increase public safety. This policy applies to both incoming and outgoing cellular calls.

Scope

This policy applies to all employees.

Policy and Procedure

1. Cell phones shall be turned off or set to silent or vibrate mode during meetings, conferences and in other locations where incoming calls may disrupt normal workflow.

2. Employees may carry and use personal cell phones while at work on a sporadic basis. If employee use of a personal cell phone causes disruptions or loss in productivity, the employee may become subject to disciplinary action per company policy.

3. Department managers reserve the right to request that the employee provide cell phone bills and usage reports for calls made during the working hours of that employee to determine if use is excessive.

4. Personal cell phones shall be used for company business on a sporadic basis. Employees may be reimbursed for the incoming calls to their personal cell phones. Employees shall not be reimbursed for outgoing calls made from their cell phones unless prior authorization is obtained from their immediate supervisor.

5. Use of the cellular phone while driving is strictly prohibited. Texting or instant messaging is also not allowed while operating a company vehicle as well. Failure to follow this policy may result in disciplinary action up to and including termination.

6. If an employee is issued a company cell phone, this may not be used for personal phone calls unless authorized by the Company prior to usage. All rules from this policy applies to company issued cell phones.

7. Any unauthorized use and/or illegal activity shall not be done in conjunction with a cellular phone whether it is company owned or personally owned. Such activities include, but are not limited to, downloads, internet usage of any kind, drug-related activities, and the like.

ELECTRONIC MAIL AND INTERNET USAGE

I. POLICY

Computers, computer files, electronic communication systems, internet access, and software furnished to employees are Company property intended to be used solely for business purposes. Any materials developed by an employee with company resources during or after normal work hours will be the property of the Company, including patentable inventions, copyrights, and trade secrets. All work done with Company resources will be owned by the Company or will be deemed assigned to the Company. Employees should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with this policy, computer, e-mail, and internet usage may be monitored.

II. ACCESS OF INFORMATION

An electronic mail system has been installed by the Company to facilitate business communications. The password to access this system belongs to the Company. This system should be treated like other shared filing systems and the Company reserves the right to access the contents of e-mail communications at all times, with or without notice, for any purpose. All system passwords and encryption keys must be available to Company management, and you may not use passwords that are unknown to your supervisor or install encryption programs without turning over encryption keys to your supervisor. All e-mail messages are Company records. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the Company without your permission. Therefore, you should not assume that messages are confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

III. E-MAIL USAGE

Because the Company provides the electronic mail system to assist you in the performance of your job, you should use it for official Company business. You may also use e-mail to communicate regarding Union issues protected under the National Labor Relations Act. Incidental and occasional personal use of e-mail is permitted by the Company, but these messages will be treated the same as other messages. The Company reserves the right to access and disclose as necessary all messages sent over its e-mail system, without regard to content.

Since your personal messages can be accessed by Company management without prior notice, you should not use e-mail to transmit any messages you would not want read by a third party. For example, you should not use the Company's e-mail for gossip, including personal information about yourself or others, for forwarding messages under circumstances likely to embarrass the sender, or for emotional responses to business correspondence or work situations.

IV. E-MAIL CONTENT

You may not use the Company's e-mail system in any way that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale. Examples of forbidden transmissions include sexually-explicit messages, cartoons, or jokes; unwelcome propositions or love letters; ethnic or racial slurs; or any other message that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs. An Employee sending any inappropriate e-mail content may be subject to discipline up to and including termination.

INTERNET ACCESS

Access to the Internet is provided for legitimate business purposes and "surfing" the net for non-business purposes during business hours is prohibited. To avoid copyright infringement claims or unlicensed use, downloading any software from the Internet without Company authorization is prohibited. Additionally, posting of copyrighted materials on the Internet for any business purpose is prohibited. Employees will be responsible for all costs arising out of the intentional improper or unlawful use or abuse of the Internet/e-mail, including attorneys fees and costs incurred.

V. SYSTEM SECURITY

Security of information is a priority. Employees with access to the Internet are expected to use extreme care in the selection and confidentiality of their password. Employees are prohibited from the unauthorized use of the passwords and encryption keys of other employees to gain access to the other employee's e-mail messages. Anyone using the e-mail system who discovers a security problem is required to notify the Systems Analyst.

VI. NOTIFICATION AND DISCIPLINARY ACTION

Employees should notify their immediate supervisor, the Human Resources Manager or any member of management upon learning of violations of this policy. Employees who violate any portion of this policy will be subject to disciplinary action, up to and including termination of employment.

MEAL BREAKS

Employees entitled to meals breaks are required to punch or sign out on their timecards for all meal or rest breaks of 30 minutes or more. Employees should observe all meal and rest breaks unless otherwise authorized by the employee's immediate supervisor. Failure to return from meal and rest breaks on time could subject the employee to disciplinary action up to and including discharge.

EMPLOYEE BENEFITS

SUMMARY OF BENEFITS
for FULL-TIME REGULAR EMPLOYEES

The Company provides, in addition to competitive wages, a wide range of benefits to help meet the needs of its employees.

This section contains brief summaries and eligibility requirements of the benefit plans which are currently part of the Company's benefit package for full-time regular employees. The summaries do not provide detailed technical and/or exhaustive explanations of the benefits available but are merely intended to provide you with general descriptions of some of the more important features of the various plans.

The Company reserves the right to amend, modify, delete and/or add to any and all terms related to these benefits without notice as it deems fit, including but not limited to, types of benefits provided, premiums and insurance.

SUMMARY OF BENEFITS
for FULL-TIME REGULAR EMPLOYEES

Full-time regular employees may be eligible to receive the following benefits according to the time schedule listed below. Please refer to the following pages to determine your eligibility and cost, if any, for these benefits. More detailed information on benefits may be obtained from the Corporate Human Resources Department.

ELIGIBILITY PERIOD	TYPE OF BENEFIT
Upon **Hire**	• Workers' Compensation Insurance • Temporary Disability Insurance • Social Security contributions • Military Service Leave without Pay • Witness/Jury Duty (without pay) • Voting Time, if applicable
Upon **completion of one month** of continuous employment	• Medical/Vision/Prescription Insurance - for Employee only • Flexible Spending Plan - Insurance Premiums Account - for Employee only
Upon **completion of three months** of continuous employment	• Dental Insurance - for Employee only • Group Life Insurance • Paid Holidays • Employee Assistance Program
Upon **completion of six months** of continuous employment	• Medical/Vision/Prescription Insurance for Dependents • Dental Insurance for Dependents • Flexible Spending Plan - Insurance Premiums Account - for Dependent coverage • Flexible Spending Plan - Medical Expense Account • Flexible Spending Plan - Dependent Care Expense Account • Voluntary Insurance Coverage
Upon **completion of a twelve month** period and **1250 hours** of service at a worksite with **50 or more employees**	• Family and Medical Leave
Upon **completion of one year** of continuous employment and **1000 hours of service**	• 401(k) Retirement Savings Plan • ROTH 401(k) Retirement Savings Plan
Upon **completion of one year** of continuous employment as a full-time regular	• Leave with Pay = 6 days • Leave without Pay • Witness/Jury Duty Leave with Partial Pay • Funeral Leave
Upon **completion of two years** of continuous employment as a full-time regular	• Leave with Pay = 12 days
Upon completion of **three or more years** of continuous employment as a full-time regular	• Leave with Pay = 18 days

NOTE: This list briefly summaries the eligibility periods for full-time regular employees of the Company. Plan documents should be consulted for all details regarding any benefit plans. The Company reserves the right to amend, modify, delete and/or add to any and all terms related to these benefits, including but not limited to, types of benefits provided, premiums and insurance, to interpret any and all provisions of the Handbook or the other plan documents, and to determine eligibility for the benefits, without notice as it deems fit.

MEDICAL INSURANCE

Full-time regular employees may participate in either of the three medical plans specified below. All plans include drug and vision riders and cover a percentage of medical, surgical, hospital, lab and professional service fees. Employee as well as dependent coverage is available. Once the employee meets the eligibility requirements, the Company pays a portion of the monthly medical premium. Information on these plans can be obtained from the Corporate Human Resources Department.

Insurers

1. HMSA Comp Med Plan
2. HMSA Preferred Provider Plan, Preferred Provider Drug Plan
3. HMSA Health Plan Hawaii Plus
4. Kaiser with Drug and Vision

Eligibility Requirements

- For Employee coverage:

  Employees are eligible for coverage when their term of employment is equal to 30 calendar days.

- To include Dependent coverage:

  Dependents are eligible for coverage when the employee's term of employment is equal to 180 calendar days.

The company does not allow medical insurance coverage for a spouse and/or dependent(s), if your spouse and/or dependent(s) are covered by another medical plan.

DENTAL INSURANCE

Full-time regular employees may participate in one of the two dental plans listed below. Both plans are provided by HMSA. Once the employee meets the eligibility requirements, the Company pays a portion of the monthly dental premium. Additional information on these plans can be obtained from the Corporate Human Resources Department.

Insurers

1. Dental L48 Plan

2. Dental HMO Plan

A detailed benefits listing may be obtained from the Corporate Human Resources Department

Eligibility Requirements

- For Employee coverage:

  Employees are eligible for coverage when their term of employment is equal to 90 calendar days.

- To include Dependent coverage:

  Dependents are eligible for coverage when the employee's term of employment is equal to 180 calendar days.

The company does not allow dental insurance coverage for a spouse and/or dependents, if your spouse and/or dependents are covered by another dental plan.

COBRA

Under the Consolidated Omnibus Budget Reconciliation Act (COBRA) employees and their dependents may elect to continue coverage under the Company's group health care plan if either the employee, spouse, or dependent children would otherwise lose coverage for certain specific reasons and do not have any other group health care plan. See the Corporate Human Resources Department for details.

PERSONAL LEAVE WITH PAY

Full-time regular employees are eligible for Leave with Pay based upon their length of employment as follows:

1 year of employment	=	6 days*
2 years of employment	=	12 days*
3+ years of employment	=	18 days*

*Personal Leave with Pay earned will be earned at the employee's current wage rate and calculated based on the average number of hours worked per day in a given week, not to exceed a maximum of eight (8) hours per day. Personal Leave with Pay will be accumulated in a dollar amount equivalent.

Employees may use their Leave with Pay for vacation and absences which occur on the employee's normal work days, or for any other personal reasons as the employee wishes. On the Request, the employee must indicate the approximate date of his/her return to work and the reasons for the Leave with Pay. The Company will try to make every effort to grant your Leave with Pay as requested. However, approval of Leave with Pay is subject to workload and staffing needs.

All employees absent or who miss work due to an emergency, must complete and submit a Leave with Pay Request to their Supervisor upon their return to work in order to be paid for such days.

Employees incurring a long-term, non-industrial injury or illness that is compensable under temporary disability insurance (TDI) will receive compensation for part of the 7-day waiting period as follows:

1 year of employment	=	3 days (or a maximum of 24 hours) paid during the waiting period
2 years of employment	=	4 days (or a maximum of 32 hours) paid during the waiting period
3+ years of employment	=	5 days (or a maximum of 40 hours) paid during the waiting period

Leave with Pay may be accumulated up to a maximum of five (5) week s which may be up to 250 hours.. At the time of the employee's anniversary date, any accumulated Leave exceeding this maximum (5 weeks or up to 250 hours) that has not been taken, will be forfeited.

Leave with Pay will not be accrued or due an employee until one (1) full year of employment as a full-time regular is completed. Subsequently, Leave with Pay is earned and calculated on each anniversary year thereafter and there is no prorating for a partial year of service. Leave with Pay will be prorated for an anniversary year *only* if an employee is granted a leave of absence *without* pay, or if an employee was employed for a full anniversary year but worked less than 1800 hours.

An employee's leave with pay is calculated on the first of the month following one's anniversary date. (An employee's anniversary date is defined as the day on which an employee's status was changed to "full-time regular.")

PERSONAL LEAVE WITHOUT PAY

A leave of absence without pay may be granted to full-time regular employees for compelling personal reasons. Personal leave without pay is not authorized to extend absences provided under the Family & Medical Leave (FMLA) benefit. A personal leave of absence without pay is defined as a period during which the employee is not working and receiving wages. Employees can take no more than two (2) leave of absences with a combined total of no more than 60 calendar days within a 365 consecutive day period. Employees requesting a Leave of Absence without pay will be required to use all accumulated Leave with Pay before taking an unpaid Leave of Absence.

Each case will be reviewed on an individual basis taking into consideration length of leave and position involved. Written request by the employee and approval by the employee's Supervisor and Subsidiary/Division Manager is required. Efforts will be made to reinstate you to the same position, if it can be held open, or if possible, to a similar position, at the end of the leave. However, this statement should not to be construed to be a guarantee of continued employment.

Company-provided benefits will cease as of the first day of the month following the effective date of your unpaid Leave of Absence. The employee may elect to continue coverage under the company's group medical and dental plans at a cost of 102% of the monthly benefit premiums. (Refer to Page D-7 for COBRA benefit.) Contact the Corporate Human Resources Department for details.

It is the employee's responsibility to notify his/her Supervisor two weeks before the end of the leave, should the expected date of return change. Failure to do so may be considered a voluntary resignation.

Eligibility Requirements

- Full-time regular employees are eligible to request a leave of absence without pay when their term of employment as a full-time regular is equal to one (1) year.

FLEXIBLE SPENDING PLAN

Full-time regular employees are eligible to participate in the Company's Flexible Spending Plan upon completion of the eligibility requirements. A "Flex Plan" enables the employee to set aside portions of their wages to pay for medical, dental, drug, vision, voluntary insurance and dependent care expenses before income and Social Security taxes are applied. The money set aside reduces the employee's taxable income so the employee pays less taxes and increases his/her net spendable income.

With the Flex Plan, the employee can pay bills with tax-free money that may be put into one or all of three separate spending accounts:

(1) Insurance Premiums Plan - The portion of the monthly insurance premiums the employee pays through payroll deduction for dependent medical and dental insurance, can be automatically paid with pretax dollars. Voluntary insurance premium plans with exception to Group Life Insurance is also eligible in the Flex Plan.

(2) Medical Expense Plan - Use this account to pay for medical, dental, drug and vision expenses that the health plan doesn't cover. This account is especially useful to employees with predictable expenses such as contact lenses, braces, maintenance drugs and medical supplies.

(3) Dependent Care Expense Plan - Employees who pay for child care services, including preschool and afterschool care can take advantage of this account. It can also be used to pay for the care of someone, child or adult, who is physically or mentally incapacitated and dependent upon the employee.

At the beginning of each plan year, the employee decides how much money, if any, he/she wants to allocate to each account by carefully estimating what his/her expenses will be for the plan year. Elections remain constant for the plan year unless there is a family status change or job status change for the employee and/or spouse including termination of spouse's employment. Each pay period, the amounts that were decided on are deducted and then allocated to individual spending accounts established especially for the employee. The flexible spending plan provider will manage each of the accounts -- all the employee does is keep track of his/her medical, dental, drug, vision and dependent care expenses.

To be reimbursed for these expenses, the employee chooses a "Benny Card" that is used like a debit card for an annual fee or the employee fills out a Reimbursement Request Form and sends it with copies of receipts to the flexible spending plan provider. A reimbursement check is then mailed directly to the employee's home. It is important that employees plan their expenses carefully since any money remaining in the employee's accounts at the end of the plan year are forfeited. Additional information on the Flexible Spending Plan can be obtained from the Corporate Human Resources Department.

Eligibility Requirements

- Insurance Premiums Plan - Employees are eligible to participate in this plan upon completion of 30 days of service. For dependent coverage, the eligibility period is extended to 180 calendar days.

- Medical Expense Plan - Employees are eligible to participate in this plan upon completion of 180 calendar days. Amount placed into the Medical Expense Plan is subject to years of service.

- Dependent Care Expense Plan - Employees are eligible to participate in this plan upon completion of 180 calendar days.

GROUP LIFE INSURANCE

Full-time regular employees may join the group life insurance plan Medical Life Insurance Company and are then provided term life insurance in the amount of one and one half (1-1/2) times their base annual salary with a maximum of $50,000 of coverage. The plan provides employees with term life and accidental death and dismemberment insurance coverage 24 hours per day. The Company pays the premium for this insurance coverage.

Eligibility Requirements:

- Employees are eligible for coverage when their term of employment is equal to 90 calendar days.

- Dependent coverage is not available.

WORKER'S COMPENSATION INSURANCE

Worker's compensation insurance is provided as required by state and federal regulations. It covers a work-related injury or illness. If you are injured, notify your Supervisor or the office management personnel immediately, but in no event later than 24 hours. Modified duty will always be available, if feasible. A written release, with physical limitations if any, by your physician is required, at the latest, on the first day you return to work. FMLA Leave and Workers Compensation will be run simultaneously.

SOCIAL SECURITY BENEFITS

The Company pays its required portion of the cost of retirement benefits provided under the federal Social Security Administration. Upon retirement, the amount of an employee's monthly benefit is determined by his level of earnings and the number of years of coverage under the plan. The range of benefits and levels of benefits are periodically adjusted by Congress.

Eligibility Requirements

- No Company eligibility requirements. Benefits are provided in accordance with governmental statutory requirements.

PAID HOLIDAYS

Full-time regular employees receive the following ten (10) paid holidays per calendar year:

New Year's Day, President's Day, Memorial Day, Kamehameha Day, Independence Day, Labor Day, Veteran's Day, Thanksgiving Day, Christmas Day, Employee's Birthday

Full-time regular employees are eligible to receive holiday pay under the following conditions:

1. When an employee's term of employment is 90 calendar days or more
2. The employee must have worked the regular scheduled work day prior to and after the holiday
3. If an employee was absent:
   a. The absence was due to an accident or illness covered by a medical doctor's disability certificate
   b. The absence was due to a pre-approved Leave of Absence Request (which includes timely notification to and approval from an employee's immediate supervisor or manager excusing the absence

An employee wishing to take a Birthday Holiday must complete a Leave of Absence Request form for their supervisor and/or Manager to approve. A birthday holiday should be taken within the month it occurs. Exceptions will be handled on a case by case basis.

If a paid holiday falls within an employee's scheduled and approved leave, it will be paid as a holiday versus vacation.

Employees will not receive Holiday with pay if the employee is eligible for or receiving the following:

1. Temporary Disability Insurance (TDI) Benefits
2. Workers Compensation Benefits
3. Unemployment Insurance Benefits

FAMILY AND MEDICAL LEAVE (FMLA)

Basic Leave Entitlement
FMLA requires covered employers to provide up to 12 weeks of unpaid, job protected leave to eligible employees for the following reasons:

- For incapacity due to pregnancy, prenatal medical care or child birth;
- To care for the employee's child after birth, or placement for adoption or foster care;
- To care for the employee's spouse, son or daughter, or parent, who has a serious health condition or
- For a serious health condition that makes the employee unable to perform the employee's job.

Military Family Leave Entitlements
Eligible employees with a spouse, son, daughter, or parent on active duty or call to active duty status in the National Guard or Reserves in support of a contingency operation may use their 12-week entitlement to address certain qualifying exigencies. Qualifying exigencies may include attending certain military events, arranging for alternative childcare, addressing certain financial and legal arrangements, attending certain counseling sessions, and attending post-deployment reintegration briefings.

FMLA also includes a special leave entitlement that permits eligible employees to take up to 26 weeks of leave to care for a covered service member during a single 12-month period. A covered servicemember is a current member of the Armed Forces, including a member of the National Guard or Reserves, who has a serious injury or illness incurred in the line of duty on active duty that may render the servicemember medically unfit to perform his or her duties for which the servicemember is undergoing medical treatment, recuperation, or therapy; or is in outpatient status; or is on the temporary disability retired list.

Benefits And Protections
During FMLA leave, the employer must maintain the employee's health coverage under any "group health plan" on the same terms as if the employee had continued to work. Upon return from FMLA leave, most employees must be restored to their original or equivalent positions with equivalent pay, benefits, and other employment terms.

Use of FMLA leave cannot result in the loss of any employment benefit that accrued prior to the start of an employee's leave.

Eligibility Requirements
Employees are eligible if they have worked for a covered employer for at least one year, for 1,250 hours over the previous 12 months, and if at least 50 employees are employed by the employer within 75 miles.

Definition of Serious Health Condition
A serious health condition is an illness, injury, impairment, or physical or mental condition that involves either an overnight stay in a medical care facility, or continuing treatment by a health care provider for a condition that either prevents the employee from performing the functions of the employee's job, or prevents the qualified family member from participating in school or other daily activities.

Subject to certain conditions, the continuing treatment requirement may be met by a period of incapacity of more than 3 consecutive calendar days combined with at least two visits to a health care provider or one visit and a regimen of continuing treatment, or incapacity due to pregnancy, or incapacity due to a chronic condition. Other conditions may meet the definition of continuing treatment.

Use of Leave
An employee does not need to use this leave entitlement in one block. Leave can be taken intermittently or on a reduced leave schedule when medically necessary. Employees must make reasonable efforts to schedule leave for planned medical treatment so as not to unduly disrupt the employer's operations. Leave due to qualifying exigencies may also be taken on an intermittent basis.

Substitution of Paid Leave for Unpaid Leave
Employees may choose or employers may require use of accrued paid leave while taking FMLA leave. In order to use paid leave for FMLA leave, employees must comply with the employer's normal paid leave policies.

Employee Responsibilities
Employees must provide 30 days advance notice of the need to take FMLA leave when the need is foreseeable. When 30 days notice is not possible, the employee must provide notice as soon as practicable and generally must comply with an employer's normal call in procedures.

Employees must provide sufficient information for the employer to determine if the leave may qualify for FMLA protection and the anticipated timing and duration of the leave. Sufficient information may include that the employee is unable to perform job functions, the family member is unable to perform daily activities, the need for hospitalization or continuing treatment by a health care provider, or circumstances supporting the need for military family leave. Employees also must inform the employer if the requested leave is for a reason for which FMLA leave was previously taken or certified. Employees also may be required to provide a certification and periodic recertification supporting the need for leave.

Employer Responsibilities
Covered employers must inform employees requesting leave whether they are eligible under FMLA. If they are, the notice must specify any additional information required as well as the employees' rights and responsibilities. If they are not eligible, the employer must provide a reason for the ineligibility.

Covered employers must inform employees if leave will be designated as FMLA-protected and the amount of leave counted against the employee's leave entitlement. If the employer determines that the leave is not FMLA-protected, the employer must notify the employee.

Unlawful Acts by Employers
FMLA makes it unlawful for any employer to:

- Interfere with, restrain, or deny the exercise of any right provided under FMLA;
- Discharge or discriminate against any person for opposing any practice made unlawful by FMLA or for involvement in any proceeding under or relating to FMLA.

Enforcement
Any employee may file a complaint with the US Department of Labor or may bring a private lawsuit against an employer.

FMLA does not affect any Federal or State law prohibiting discrimination, or supersede any State or local law or collective bargaining agreement which provides greater family or medical leave rights.

Uniformed Services Employment And Reemployment Rights Act (USERRA)

USERRA protects the job rights of individuals who voluntarily or involuntarily leave employment positions to undertake military service or certain types of service in the National Disaster Medical System. USERRA also prohibits the Company from discriminating against past and present members of the uniformed services, and applicants to the uniformed services.

The Company will provide its employees the benefits and rights afforded under the Uniformed Services Employment and Reemployment Rights Act of 1994. An employee's rights under this policy will be terminated if the employee is: (1) separated or dismissed from service with a dishonorable or bad conduct discharge; (2) discharged under other than honorable conditions; or (3) dropped from the rolls of the uniformed service before satisfactory completion of the employee's term of service.

Employee Status And Entitlements While Performing Military Service. Employees called to duty in the uniformed services, including duty with the National Guard, the Reserves or the Public Health Service, will receive authorized military absence without pay. Employees performing duty with a uniformed service will be entitled to reemployment rights and other benefits if:

(1) They give their Supervisor advanced written or verbal notice of their intention or obligation to perform the service requiring their absence; and

(2) The cumulative length of the absence plus all prior absences from the Company on military service leave does not exceed five (5) years.

Notice And Requests For Military Leave. To avoid disruption in Company operations, the Company requests that employees complete a Leave of Absence Request and give it to the Corporate Human Resources Department at least two (2) weeks prior to the absence period.

The Leave of Absence form should indicate the beginning date of the leave, the anticipated duration, and the expected date of return to work. In addition, the employee should attach to the Leave of Absence form a copy of the official military orders directing the military duty.

Return To Work. Employees returning to work with the Company must comply with the following return times:

(1) For Absences of less than 31 days. The employees must report to the Corporate Human Resources Department and apply for return to work not later than the first regularly scheduled work shift on the day after completion of uniformed service. (The employee will be permitted sufficient time for safe travel from their duty site to home plus eight hours).

(2) For Absences of more than 30 days but less than 181 days. The employee must report to the Corporate Human Resources Department and apply for return to work not later than 14 days after completion of uniformed service.

(3) For Absences of more than 180 days. The employee must report to the Corporate Human Resources Department and apply for return to work not later than 90 days after the completion of uniformed service.

Reemployment Benefits and Positions. Unless the Company circumstances have so changed as to make reemployment impossible or unreasonable, the Company will provide reemployment opportunities outlined below to employees returning from uniformed service. In addition, the Company will afford a returning employee the seniority ranking and benefits that the employee would have received if his or her continuous employment had not been interrupted by uniformed service.

The Company will place employees returning from military leave in positions according to the following scheme:

(1) For absences of less than 91 days. The employee will be placed in the position in which he or she would have been employed if uniformed service had not interrupted the employee's continuous employment. If the position is different from the position the employee left to perform uniformed service, the Company will make reasonable efforts to qualify the employee for the new position. If after reasonable efforts, the employee is not qualified for the new position, the Company will return the employee to the position he or she filled at the time of departure on military leave.

(2) For absences of more than 90 days. The employee will be placed in the position in which he or she would have been employed if uniformed service had not interrupted the employee's continuous employment or a position of like seniority, status, and pay. If the employee is not qualified to perform the duties of this position, the Company will make reasonable efforts to qualify the employee for the position.

If after reasonable efforts the employee does not qualify for the new position, the Company will place the employee in the position the employee left to perform uniformed service. If that position is not available, the Company will place the employee is a position the employee is qualified to perform and is of like seniority, status and pay as the position the employee left to perform uniformed service.

WITNESS / JURY DUTY LEAVE

A leave of absence with partial pay will be granted to you if you are summoned to serve as a juror or witness as prescribed by law. During the first five (5) days you are on jury or witness duty, the Company will pay you the difference between the amount to you receive from jury duty or as a witness (excluding travel/mileage reimbursement) and your regular straight time pay. If your jury or witness duty lasts beyond five (5) days, you may take Leave with Pay or you will receive a Leave of absence without Pay for the remainder of your service.

If you are serving as a juror, you must submit to your Supervisor a proper certification from a court official indicating the time you spent on jury duty and the amount of jury fees you received. If you are summoned to serve as a witness in a case, you must submit to your Supervisor a copy of the subpoena you received and the amount of witness fee you received. Employees on jury or witness duty will receive full service credits and privileges during the entire period they are on jury or witness duty.

Eligibility Requirements

- Full-time regular employees are eligible for witness / jury duty leave with partial pay when their term of employment is equal to one (1) year.

FUNERAL LEAVE

A funeral leave with pay is available to all full-time regular employees for the loss of a member of their immediate family, defined as spouse, children, father, mother, sister, brother, grandfather, grandmother, father-in-law, mother-in-law, grandparents-in-law. An employee will receive a leave with pay of up to three (3) days per fiscal year to make funeral arrangements or attend services.

Eligibility Requirements

- Full-time regular employees are eligible for funeral leave when their term of employment is equal to one (1) year.

401(k) RETIREMENT SAVINGS PLAN
ROTH 401(K) RETIREMENT SAVINGS PLAN

The Company offers full-time employees the opportunity to start a retirement savings fund through the Unitek 401(k) Retirement Savings Plan or Roth 401(k) upon completion of the eligibility requirements. Employees are encouraged to participate in this plan by contributing part of their compensation into the plan where it is invested per direction of the employee. Gains on these contributions are also tax deferred until funds are distributed to the employee. Participants are allowed to contribute the lesser of 15% of their gross salary or the varying annual Internal Revenue Service limit per calendar year. The Company may elect to match employee contributions with additional company funds. Additionally, the Company may annually contribute a portion of its net profits into the plan. All plan accounts are 100% vested at all times. Funds that are added at the company's discretion will have a 5 year vesting period. Additional information on the 401(k) Retirement Savings Plan or Roth 401(k) can be obtained from the Corporate Human Resources Department.

Eligibility Requirements

- Employees are eligible to participate in either of the Retirement Savings Plan upon completion of one (1) full year (365 days) of employment with a minimum of 1000 hours of service within that period.

EMPLOYEE ASSISTANCE PROGRAM (EAP)

Full-time regular employees are eligible to participate in the company-sponsored employee assistance program (EAP). This program is designed to help employees and their families resolve personal problems (e.g. physical illness, emotional problems, family and marital conflicts, alcohol and drug problems, financial stress and legal problems) before they adversely affect the employee's health, happiness and ability to perform their job. Confidential and professional counseling assistance is currently provided by Work Life Hawaii (808-543-8445 or Toll Free 24 hours/7 days a week 800-994-3571). Additional information about the Company's Employee Assistance Program can be obtained from the Corporate Human Resources Department.

Eligibility Requirements

- Full-time employees are eligible to utilize the services of this program when their term of employment is equal to 90 calendar days.

VOTING TIME

The Company encourages employees to register and vote in the Primary, General, or Special Elections. If you are unable to vote before or after your normal working hours on election day, you may request and obtain time off, up to a maximum of two consecutive (2) hours with pay for voting time. To ensure the Company can properly schedule workers for ongoing work requirements, you must schedule voting time with your supervisor at least one (1) week prior to election day.

Employees who are granted time off to vote during their normal hours are required to produce a voter receipt to their supervisor upon their return from voting. Employees who take time off but fail to vote will not be paid for such time off.

Eligibility Requirements

- No Company eligibility requirements. Benefits are provided in accordance with governmental statutory requirements.

SUMMARY OF BENEFITS
for FULL-TIME TEMPORARY and PART-TIME EMPLOYEES

Full-time temporary and Part-time employees may be eligible to receive the following benefits according to the time schedule listed below. Please refer to the following pages to determine your eligibility and cost, if any, for these benefits. More detailed information on benefits may be obtained from the Corporate Human Resources Department.

ELIGIBILITY PERIOD	TYPE OF BENEFIT
Upon **Hire**	• Workers' Compensation Insurance • Temporary Disability Insurance • Social Security contributions • Military Service Leave without Pay • Witness/Jury Duty • Voting Time
Upon **completion of four consecutive weeks consisting of 20 hours** of work	• Medical Insurance - for Employee only
Upon **completion of three months** of continuous employment	• Employee Assistance Program
Upon **completion of a twelve month** period and **1250 hours** of service at a worksite with **50 or more employees**	• Family and Medical Leave
Upon **completion of one year** of continuous employment and **1000 hours of service**	• 401(k) Retirement Savings Plan
Upon **completion of one year** of continuous employment	• Leave without Pay

NOTE: This list briefly summaries the eligibility periods for full-time temporary and part-time employees of the Company. Plan documents should be consulted for all details regarding any benefit plans. The Company reserves the right to amend, modify, delete and/or add to any and all terms related to these benefits, including but not limited to, types of benefits provided, premiums and insurance, to interpret any and all provisions of the Handbook or the other plan documents, and to determine eligibility for the benefits, without notice as it deems fit.

Exhibit 2

ACKNOWLEDGEMENT OF EMPLOYEE HANDBOOK

I hereby acknowledge receipt of the Navatek Lifting Body Technologies, LLC. (Navatek LBT) Employee Handbook. I understand that the handbook is merely a general overview of some of Navatek LBT's Human Resources policies, benefits and procedures which are subject to modification, discontinuation or change which I agree to conform to the rules and regulations of Navatek LBT.

I also understand and agree that the language in the Handbook is not intended to create a contract or agreement between Navatek LBT and myself and that my employment is for no fixed term and may be terminated, with or without cause or notice, at any time, at the option of Navatek LBT or myself. I understand that no person other than the President of Navatek LBT has the authority to enter into any written or oral employment contracts or agreements on behalf of Navatek LBT.

I further understand that it is my responsibility to read the policies and procedures within this Handbook. I also understand that it is my responsibility to return this Handbook prior to or on my last day of employment.

Martin Kao
Print Name

Signature

Date

Exhibit 2

Exhibit 3

Martin Defense Group

Information System Security Policies and Procedures Manual

Exhibit 3

Approved by:

_____ _____

Daniel Brunk Date
Martin Defense Group LLC Chief Executive Officer

_____ _____

Eric Schiff Date
Senior VP Administration and Operations

RECORD OF CHANGES

Change No.	Date	Brief Description
—	10/28/2019	Original Issue
1	3/15/2021	Updated policies

1 Introduction

As a contractor doing business with the U.S. Department of Defense, Martin Defense Group receives and generates, in the course of our work, information (data) that is considered sensitive with negative implications for national defense should it be disclosed to unauthorized parties.

Executive Order 13556, dated November 4, 2010, established a uniform program for managing sensitive information that requires safeguarding or dissemination controls but doesn't meet the standard for classification. This program defined such information as Controlled Unclassified Information (CUI) and designated the National Archives and Records Administration as the Executive Agent to implement the program and to oversee agency actions to ensure compliance.

As part of its mandate, NARA developed a "CUI Registry,"[1] defining 24 discrete categories of CUI, as shown in the following table:

	Category		Category
1	Agriculture	13	Legal
2	Controlled Technical Information	14	Natural and Cultural Resources
3	Critical Infrastructure	15	North Atlantic Treaty Organization
4	Emergency Management	16	Nuclear
5	Export Control	17	Patent
6	Financial	18	Privacy
7	Geodetic Product Information	19	Procurement and Acquisition
8	Immigration	20	Proprietary Business Information
9	Info Systems Vulnerability Information	21	SAFETY Act Information
10	Intelligence	22	Statistical
11	International Agreements	23	Tax
12	Law Enforcement	24	Transportation

In 2016, the Department of Defense amended the Defense Federal Acquisition Regulation Supplement (DFARS) to provide for the safeguarding of controlled unclassified information when residing on or transiting through a contractor's internal information system or network. DFARS Clause 252.204-7012, Safeguarding Controlled Unclassified Information and Cyber Incident Reporting, requires contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations to safeguard Controlled Unclassified information that is processed or stored on their internal information system or network. This is included in all contracts awarded by DoD, and, as a DoD contractor, we are bound by its terms.

[1] The CUI Registry is found at https://www.archives.gov/cui/registry/category-list.

The two principal elements of this DFARS clause concern *adequate security* and *cyber incident reporting*. These require, in part, that contractors implement the security requirements in NIST SP 800-171, and that cyber incidents affecting a covered contractor information system, or the Controlled Unclassified information residing therein, must be reported to DoD within 72 hours of discovery.

2 Purpose

The purpose of this manual is to establish a comprehensive set of policies and procedures that enable Martin Defense Group to comply with the requirements of DFARS Clause 252.204-7012 for providing adequate security for CUI and for cyber incident reporting.

3 Scope

The policies and procedures set forth herein apply to all Martin Defense Group Users and its subsidiaries.

4 Organization

This manual comprises the preceding introductory material and the following sections containing the policies and procedures, respectively, that govern the implementation and use of Martin Defense Group's information system.

5 Key Roles and Responsibilities

The following key roles perform a variety of functions that are specified throughout this manual. Where appropriate, a single individual may fulfill multiple roles.

- Senior Management Official (SMO). The SMO is the "owner" of Martin Defense Group's information system, performing executive-level functions. Specific responsibilities are given in the relevant individual policies.
- System/Network Administrator. Administers the information system on behalf of the SMO. Specific responsibilities are given in the relevant individual policies.
- Account Managers. Approve new information system accounts, set and change account privileges, and terminate accounts. Generally, each Account Manager is responsible for the accounts of personnel in their respective reporting chains.
- Audit Administrator. Performs essential information system security audit functions on behalf of the SMO. Specific responsibilities are given in the relevant individual policies.
- Facility Security Officer (FSO). The FSO supervises and directs security measures necessary for implementing applicable requirements of the National Industrial Security Program at Martin Defense Group and is assigned specific roles for information system security.

Acceptable Use Policy

1 Overview

Internet/Intranet-related systems at Martin Defense Group LLC (Martin Defense Group), including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail and internet access, are the property of Martin Defense Group. These systems are to be used for business purposes in serving the interests of the organization, and of our clients and customers in the course of normal operations. Please review Human Resources policies for additional guidance.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

2 Purpose

The purpose of this policy is to outline the acceptable use of information systems at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Inappropriate use exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to access Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

4 Policy

4.1 General Use and Ownership

a. Martin Defense Group sensitive information stored on electronic and computing devices whether owned or leased by Martin Defense Group, a User, or a third party, remains the sole property of Martin Defense Group. You must ensure through legal or technical means that sensitive information is protected in accordance with NIST SP 800-171[2].

b. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Martin Defense Group proprietary information.

[2] National Institute of Standards and Technology Special Publication 800-171, Rev 1, published 7-June 2018, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

c. Users may access, use or share Martin Defense Group proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

d. Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty regarding a particular use, Users should consult their supervisor or manager.

e. For security and network maintenance purposes, Designated IT Personnel will monitor equipment, systems, and network traffic at any time, per Martin Defense Group's Monitoring and Systems/Communications Protection Policy.

f. Martin Defense Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

g. Users will only use the appropriate login or set of system permissions to perform their tasks, per Martin Defense Group's Access Control Policy. For instance, Designated IT Personnel shall not perform non-system-administrator tasks while logged in as a system administrator. (3.1.4, AC-5)[3]

h. Users may not change the configuration of their workstation or laptop without authorization from Designated IT Personnel (see Martin Defense Group's Configuration Management policy).

4.2 Security Training

Adequate training in security procedures is an essential element of overall security. As such, Martin Defense Group:

a. Ensures that Users are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems before being authorized to access the system, and that they receive security awareness training at least annually and when required by security changes. (3.2.1, AT-2a, AT-2b, AT-2c)

b. Ensures that Users are adequately trained to carry out their assigned information security-related duties and responsibilities, and that they receive security-related duty and responsibility training at least annually and when required by security changes. (3.2.2, AT-3a, AT-3b, AT-3c)

c. Provides security awareness training on recognizing and reporting potential indicators of insider threat. (3.2.3, AT-2 (2))

4.3 Safe Controlled Unclassified Information (CUI) Management

Controlled unclassified information (CUI) must be protected from disclosure. Further, CUI must be protected when it is sent outside a CUI-safe network and also when it is stored on removable media. As such:

a. Users may only store CUI on a computer that is designated as a CUI computer and:

[3] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., "3.1.1") and/or NIST SP 800-53 (beginning with a letter, e.g., "AC-2").

1. The computer is currently in a specific CUI-safe network, or
2. The computer is completely unattached from any networks, or
3. The computer is connected to a CUI-safe network through a Martin Defense Group-approved VPN.

b. Users may only send CUI over networks that are not CUI-safe if the CUI is first encrypted with FIPS 140-2 level encryption. This includes, but is not limited to, sending data via email or web browser. Address any questions regarding the safety of a specific network to Designated IT Personnel.

c. Users may only store CUI on removable media if the media is owned by the company, has been scanned for viruses and malware, and the CUI has been encrypted with FIPS 140-2 level encryption (see Media Protection and Backup Policy).

d. Once CUI has been removed from removable media, the media must be sanitized (see Media Protection and Backup Policy).

e. CUI may be stored on notebook/laptop computers in accordance with section 4.3.a.

f. CUI may not be stored on mobile computing devices other than laptops and encrypted company-issued cellphones.

4.4 Remote Access and CUI

Systems containing CUI must be protected from unauthorized access. Before allowing or starting remote connections to Martin Defense Group systems, review the following policies:

- Access Control Policy (remote sessions must be authorized, monitored and controlled, use cryptographic mechanisms, and be routed via managed access control points).
- Monitoring and System/Communications Protection Policy (prevent split-VPNs and remote activation of collaborative computing devices and provide an indication when collaborative computing devices are in use).

4.5 Safe System/Internet Use

a. Before opening email attachments received from untrusted sources, Users must first ensure such attachments are free from malware, etc., by using anti-virus tools provided by the organizational system.

b. If there is a need to access untrusted websites blocked by Martin Defense Group's information system, Users should contact Designated IT Personnel to obtain access.

4.6 Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from some of these restrictions during the course of their legitimate job responsibilities (e.g., Designated IT Personnel may have a need to disable the network access of a host if that host is disrupting business operations). These lists are by no means exhaustive but provide a framework for identifying activities that constitute an unacceptable use.

a. Under no circumstances is a User authorized to engage in any activity that is illegal under local, state, federal or international law while using Martin Defense Group-owned resources.

b. **Unacceptable Use - System and Network Activities**. The following activities are prohibited:

1. Providing system access to another individual through a User's account, either deliberately or through failure to secure its access.
2. Transmission of unencrypted CUI over non-CUI-safe networks via email, HTTP, and any other applications or protocols. (3.13.8, 3.13.11, SC-8, SC-8 (1), SC-13)
3. Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Martin Defense Group.
4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which Martin Defense Group or the User does not have an active license.
5. Accessing data, a server or an account for any purpose other than conducting Martin Defense Group business, even if a User has authorized access. However, incidental personal use of Martin Defense Group's information system is permissible so long as:
    i. It does not consume more than a trivial amount of resources;
    ii. It does not interfere with staff productivity;
    iii. It does not preempt any business activity.

    Use of Martin Defense Group's systems for malicious or illegal purposes or commercial activities outside the business objectives of Martin Defense Group, as noted elsewhere in this policy, is strictly prohibited.
6. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. Consult appropriate management personnel prior to the export of any material that is in question.
7. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
8. Revealing your account password to others or allowing your account to be used by others. This includes family and other household members when work is being done at home.
9. Using a Martin Defense Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
10. Making fraudulent offers of products, items, or services originating from any Martin Defense Group account.
11. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which a User is not an intended recipient, or logging into a server or account that a User is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
13. Port scanning or security scanning is expressly prohibited unless prior arrangements are made with the appropriate IT personnel.
14. Executing any form of network monitoring that will intercept data not intended for a User's host, unless this activity is a part of the User's normal job/duty.
15. Circumventing User authentication or security of any host, network, or account.
16. Introducing honeypots, honeynets, or similar technology on the Martin Defense Group network.
17. Interfering with, or denying service to, any user (for example, denial of service attack).
18. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
19. Providing information about, or lists of, Martin Defense Group employees to parties outside Martin Defense Group for non-business purposes.

c. **Unacceptable Use - Email and Communication Activities**. When using Martin Defense Group resources to access and use the Internet, including the electronic mail (email) system, Users must realize they represent Martin Defense Group in doing so. While incidental and occasional personal use of email is permitted by the Company, in such use whenever Users state an affiliation to Martin Defense Group, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of Martin Defense Group." Questions should be addressed to the User's supervisor or manager.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals, whether internal or external to Martin Defense Group, who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text message, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of social media accounts.

d. **Unacceptable Use - Blogging and Social Media**. Blogging and social media posting by Users, whether using Martin Defense Group's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Martin Defense Group's systems to engage in blogging or posting on social media (online activity) outside of normal business hours is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Martin Defense Group's policy, is not detrimental to Martin Defense Group's best interests, and does not interfere with a User's regular work duties. Blogging and social media posting from Martin Defense Group's systems is also subject to monitoring.

1. Users are prohibited from revealing any Martin Defense Group confidential or sensitive information, or trade secrets.
2. Users shall not engage in any online activity that may harm or tarnish the image, reputation and/or goodwill of Martin Defense Group, its partner organizations, and/or any of its employees. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when engaged in an online activity or otherwise engaging in any conduct prohibited by Martin Defense Group's non-discrimination and anti-harassment policy.
3. Users may not attribute personal statements, opinions, or beliefs to Martin Defense Group when engaged in online activity. If a User is expressing his or her beliefs and/or opinions in blogs or social media posts, the User may not, expressly or implicitly, represent himself or herself as an employee or representative of Martin Defense Group. Further, such postings by Users from a Martin Defense Group email address to newsgroups, blogs, or social media shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Martin Defense Group. Users assume any and all risk associated with non-business online activities.
4. In addition to complying with all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Users may not use Martin Defense Group's trademarks, logos, and any other Martin Defense Group intellectual property in connection with any non-business online activities.

Access Control Policy

5 Overview

Properly managing access to organization information systems is a critical component of information security. Controlling access to systems and data reduces the potential for harming Martin Defense Group LLC (Martin Defense Group) through data theft, malware installation, and system damage. To that end, access to organization systems, including but not limited to laptop computers, desktop computers, servers, and network devices, is to be managed according to rules outlined in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

6 Purpose

The purpose of this policy is to outline the required and acceptable methods for controlling access to information systems at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding access controls exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

7 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to access Martin Defense Group computers and systems following Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

8 Policy

8.1 Access Control

a. Martin Defense Group:

1. Limits system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). (3.1.1)[4]

    i. The Senior Management Official (SMO) identifies and selects the following types of information system accounts to support organizational

[4] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

missions/business functions: system/network administrator, audit administrator, incident response, the user (AC-2a)

ii. The SMO assigns account managers for information system accounts. (AC-2b)

iii. Conditions for group and role membership are established as follows: (AC-2c)

1. The system/network administrator group shall only have personnel who have been authorized to handle Controlled Unclassified Information (CUI) and are assigned to the administration of host and network devices.
2. The audit administrator group shall only have personnel who have been cleared to handle CUI and are assigned to administer the audit function of the system.
3. The incident response group shall only have personnel who have been cleared to handle CUI and are assigned to Martin Defense Group's Incident Response Team.
4. The user group shall only have personnel who have been approved to handle CUI.

iv. Account managers specify authorized users of the information system, group, and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. (AC-2d)

1. System/Network administrator privileges – Administrative rights (except for audit file access and management) on appropriate host and network devices.
2. Audit administrator privileges – Administrative rights for audit file access and management on appropriate host and network devices.
3. Incident response privileges – Administrative read rights for all system and log information on all system components.
4. User privileges – User rights to read/execute appropriate system information and read/write/execute access for all user-created documents on appropriate host devices.

v. Account managers approve requests to create information system accounts. (AC-2e)

vi. Designated IT Personnel create, enable, modify, disable, and remove information system accounts following procedures or conditions defined in SOP MDG-AC-100. (AC-2f)

vii. Designated IT Personnel monitor the use of information system accounts for indicators of compromise. (AC-2g)

viii. Account managers notify administrators:

1. When accounts are no longer required. (AC-2h.1)

2. When Users are terminated or transferred. (AC-2h.2)
3. When individual information system usage or need-to-know changes. (AC-2h.3)

ix. Account managers authorize access to the information system based on:

1. A valid need for access. (AC-2i.1)
2. Intended system usage. (AC-2i.2)
3. Other attributes as required by the organization or associated missions/business functions. (AC-2i.3)

x. The Audit Administrator reviews accounts for compliance with account management requirements at least annually. (AC-2j)

1. Validate authorized users of the information system.
2. Appropriate assignment of users to Group and Role membership.
3. Appropriate access authorizations/privileges for each account.
4. Required specialized training for accounts, as relevant.
5. Appropriate removal or deactivation of information system accounts.

xi. Shared/group account credentials (if deployed) will be reissued by hand delivery by Designated IT Personnel when Users are removed from the group. (AC-2k)

xii. Account managers authorize remote access to the information system before allowing such connections. (AC-17b)

2. Limits system access to the types of transactions and functions that Users are permitted to execute. (3.1.2)

i. The information system enforces approved authorizations for logical access to information and system resources following the access control policies specified herein. (AC-3)

ii. Remote access usage restrictions, configuration/connection requirements, and implementation guidance are established as follows. (AC-17a)

1. Remote administration.

a. Usage Restrictions.

i. The connection must not be initiated in a generally-accessible open area where unknown personnel can observe the screen and actions of the person connecting to the system.

ii. The connection shall only be for business purposes.

b. Configuration/connection requirements and implementation guidance.

i. Must use organization-provided Internet Protocol Security (SSL VPN) client to connect to the CUI-safe network.

ii. For laptop-type devices, if CUI data is downloaded to the device then it must be encrypted on the drive using FIPS-140-2 certified modules

iii. For tablet and phone type devices, Martin Defense Group does not allow unencrypted CUI to be downloaded to these types of devices as a matter of policy.

2. Remote user connections. Same usage restrictions, configuration/connection requirements, and implementation guidance as for remote administration.

3. Controls the flow of CUI following approved authorizations. (3.1.3, AC-4)

4. Separates the duties of individuals to reduce the risk of malevolent activity without collusion. (3.1.4)

   i. The organization separates the System/Network Administrator and Audit Administrator and documents the separation of duties of individuals. (AC-5a)

   ii. Defines information system access authorizations to support the separation of duties as defined in Section 4.1.a.1 for the System/Network Administrator and Audit Administrator. (AC-5c, AC-5b)

5. Employs the principle of least privilege, including for specific security functions and privileged accounts. (3.1.5)

   i. The organization only authorizes access for Users (or processes acting on behalf of Users) as necessary to accomplish assigned tasks following organizational missions and business functions. (AC-6)

   ii. The organization explicitly authorizes access to all security functions and security-relevant information. (AC-6(1))

   iii. The organization restricts privileged accounts on the information system to system/network and audit administrators. (AC-6(5))

6. Requires that users of information system accounts, or roles, with access to privileged security functions, use non-privileged accounts, or roles when accessing nonsecurity functions. (3.1.6, AC-6(2)) Nonsecurity functions include reading e-mail and surfing the Internet.

7. Authorizes remote execution of privileged commands and remote access to security-relevant information only for system and/or network administration needs. (3.1.15, AC-17(4)a)

   i. Privileged commands are all those commands configured to be accessible only to an administrator.

ii. Security-relevant information includes log entries and system settings implementing policy.

8. Controls wireless access to the information system. (3.1.16, AC-18b)
    i. Wireless access usage restrictions, configuration/connection requirements, and implementation guidance are established as follows. (AC-18a)
        1. Usage restrictions. Limited only to personnel that would/should have access to CUI through account manager authorization and issuance of select computers preconfigured for such purposes by Designated IT Personnel.
        2. Configuration/connection requirements. Use encryption.
    ii. Account managers authorize wireless access to the information system before allowing such connections. (AC-18b)
    iii. External users may be provided passwords by Designated IT Personnel to allow their devices to access Martin Defense Group's WIFI and connect to the Internet, but such accounts will not enable such users to access Martin Defense Group's information system.
9. Protects wireless access to the information system using authentication and encryption. (3.1.17, AC-18(1))
10. Controls the connection of mobile devices to the information system. (3.1.18, AC-19)
    i. Usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices are established as follows:
        1. Usage restrictions. Downloading unencrypted CUI to mobile devices is prohibited (see also Section 4.a.2).
        2. Configuration/connection requirements. Use FIPS 140 encryption and a password consistent with Martin Defense Group's password policy.
        3. Implementation guidance. Load the VPN client to encrypt information from the device to the CUI system.
    ii. Account managers authorize the connection of mobile devices to organizational information systems before allowing such connections.
11. Encrypts CUI on mobile computing platforms (notebook/laptop computers/encrypted company-issued cellphones); see also Acceptable Use Policy. (3.1.19, AC-19(5))
12. Verifies and controls/limits connections to and use of external systems. (3.1.20)
    i. The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
        1. Access the information system from external information systems. (AC-20a)

2. Process, store, or transmit organization-controlled information using external information systems. (AC-20b)

ii. The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system. (AC-20 (1), AC-20 (1)(b))

1. Users are prohibited from using all file-sharing services except for the following:

a. Microsoft OneDrive

b. secure.mdefensegroup.com. Only when necessary to share information with external users.

13. Limits by restriction to specific individuals the use of organizational portable storage devices on external systems. (3.1.21, AC-20(2))

14. Prohibits posting or processing CUI on publicly-accessible Martin Defense Group information systems; reviews the proposed content of information before posting onto publicly-accessible information systems, which include our public website, social media accounts (LinkedIn, YouTube), and job application website, to ensure that nonpublic information is not included. (3.1.22, AC-22c).

b. The information system:

1. Prevents non-privileged users from executing privileged functions, to include disabling, circumventing, or altering implemented security safeguards/countermeasures, and audits the execution of such functions. (3.1.7, AC-6(10), AC-6(9))

2. Limits unsuccessful logon attempts (3.1.8)

i. Enforces a limit of five (5) consecutive invalid login attempts by a user during a 15-minute time period. (AC-7a)

ii. Automatically locks the account/node for at least 15 minutes, or until unlocked by an administrator, when the maximum number of unsuccessful attempts is exceeded. (AC-7b)

3. Provides privacy and security notices consistent with applicable CUI rules. (3.1.9)

i. Displays a banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Information system usage may be monitored, recorded, and subject to audit. (AC-8.a2)

2. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties. (AC-8.a3)

3. The use of the information system indicates consent to monitoring and recording. (AC-8.a4)

   Banner: ATTENTION… ATTENTION…. This is a restricted use system. All actions performed by a user may be monitored, recorded, and are subject to audit. Any unauthorized use of this system is prohibited and may be subject to criminal and civil penalties. The use of this information system indicates consent to the monitoring and recording implemented by the system.

ii. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system. (AC-8b)

4. Uses session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity (3.1.10)
   i. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from the user. (AC-11a)
   ii. Retains the session lock until the user reestablishes access using established identification and authentication procedures. (AC-11b)
   iii. Conceals, via the session lock, information previously visible on the display with a publicly-viewable image. (ACC-11(1))
5. Automatically terminates application-level user sessions after a specific period of inactivity as follows (3.1.11, AC-12):
   i. Remote Desktop Protocol (RDP) sessions: 15 minutes.
   ii. Secure Shell (SSH) sessions: 15 minutes.
6. Employs automated monitoring and control of remote access sessions. (3.1.12, AC-17(1))
7. Employs cryptographic mechanisms to protect the confidentiality of remote access sessions. (3.1.13, AC-17(2))
8. Routes remote access via managed access control points. (3.1.14, AC-17(3))

8.2 Identification and Authentication

a. The information system:

1. Identifies system users, processes acting on behalf of users, or devices. (3.5.1, IA-2)
2. Authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. (3.5.2)

3. Uses multifactor authentication[5] for local and network access[6] to all accounts (3.5.3, IA-2 (1), IA-2 (2), IA-2 (3))
4. Employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. (3.5.4, IA-2 (8), IA-2 (9))
5. Prevents reuse of identifiers. (3.5.5, IA-4d)
6. Disables identifiers after 30 days of inactivity for all user accounts except for designated maintenance accounts that may be infrequently accessed. (3.5.6, IA-4e)
7. Enforces a minimum password complexity of a case-sensitive, 12-character mix of upper case letters, lower case letters, numbers, and special characters, and a change of at least one of the characters when new passwords are created. (3.5.7, IA-5 (1)(a), IA-5 (1)(b)) (NIST SP 800-63b)
8. Prohibits password reuse for a minimum of one (1) generation (does not apply to one-time use passwords). (3.5.8, IA-5(1)(e))
9. Requires that passwords be changed every 60 days. (IA-5g)
10. Allows temporary password use for system logins with an immediate change to a permanent password. (3.5.9, IA-5 (1)(f))
11. Stores and transmits only cryptographically-protected passwords. (3.5.10, IA-5 (1)(c))
12. Obscures feedback of authentication information. (3.5.11, IA-6)

b. Martin Defense Group:

1. Manages information system identifiers by (IA-4)
    i. Receiving authorization from an account manager to assign an individual, group, role, or device identifier. (IA-4a)
    ii. Selecting an identifier that identifies an individual, group, role, or device. (IA-4b)
    iii. Assigning the identifier to the intended individual, group, role, or device. (IA-4c)

---

[5] *Multifactor authentication* requires two or more different factors to achieve authentication. The factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

[6] *Local access* is any access to a system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. *Network access* is any access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

2. Manages information system authenticators by:
    i. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator. (IA-5a)
    ii. Default passwords for the initial login to the system shall be a randomly-generated word or phrase as determined by Designated IT Personnel. (IA-5b)
    iii. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. Initial authenticator distribution shall be accomplished either face to face or over the phone via voice or text. (IA-5d)
    iv. Changing the default content of authenticators before information system installation. (IA-5e)
    v. Protecting authenticator content from unauthorized disclosure and modification. (IA-5h)
    vi. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators. (IA-5i)
    vii. Changing authenticators for group/role accounts when membership to those accounts changes. (IA-5j)

8.3 Policy on Publicly Accessible Website

a. The IT Steering Committee is responsible for the development and administration of Martin Defense Group's public affairs policies and procedures as follows:
    1. Administer and update the policy as outlined in this instruction.
    2. Administer and maintain the Martin Defense Group website for the posting of appropriate Martin Defense Group LLC information and images.
    3. Maintain overall cognizance for Martin Defense Group website content as it pertains to the appropriateness of publicly accessible material.
    4. Maintain overall cognizance for questions about the Martin Defense Group website as it pertains to the security of computer operations or classified information.
    5. Establish a mechanism for receiving and reviewing all requests for Martin Defense Group information.

b. The Audit Administrator is responsible for the following:
    1. Conduct assessments of the Martin Defense Group website at least annually to ensure compliance with information assurance and security policy requirements.
    2. Notify the responsible parties when a site is discovered to be non-compliant to ensure the site is either removed from the world wide web or brought into compliance.

c. Martin Defense Group staff or contractors that maintain the publicly accessible Martin Defense Group website shall:
    1. Ensure all information currently residing on the website is reviewed by the public affairs officer, and the FSO is accurate and is appropriate for viewing by a worldwide

audience, friend and foe alike. Information not suitable for a publicly accessible website must be removed.

2. Develop local procedures for the approval of information posted on the website. At a minimum, Martin Defense Group's public affairs officer, in conjunction with information assurance personnel, or those at the next appropriate level to ensure posted information meets requirements.
3. Designate, in writing, a primary website manager, who may be known as the Webmaster. Contact information for the Webmaster (e.g., email address) will be included in the companies "home page" source code. At a minimum, the Webmaster shall:
    i. Have access to and be familiar with currently applicable instructions, notices, and rules regulating the content of the Martin Defense Group publicly accessible website and shall be conversant in the provisions of these directives.
    ii. Serve as the principal point of contact on all matters about the administration of the publicly accessible website.
    iii. Oversee Martin Defense Group's website and ensure compliance with current directives. Oversight includes monitoring the site as often as possible to ensure no unauthorized changes have occurred.
    iv. Register the Martin Defense Group website with required government agencies if required. Martin Defense Group will review and update their registration yearly or whenever there is a change in any of the registration data fields.

d. Administration of website

1. The Martin Defense Group website must have an articulated purpose, approved by the management, and supporting the company activity's core competency mission.
2. Only unclassified material that is approved for public release may appear on a publicly accessible website.
3. A designation of "Unofficial" is not recognized for the Martin Defense Group website. Any website created by Martin Defense Group constitutes an official website and is subject to this instruction.
4. The Martin Defense Group website must be protected from modification on systems exposed to public networks.
5. All company/activity home pages -- the logical entry point of the company/activity website -- must contain, at a minimum, the following:
    i. Full organizational name and official postal mailing address.
    ii. A statement that the site is an official Martin Defense Group website.
    iii. A prominently displayed hypertext link to a tailored Privacy Policy on the home page. All references to the Privacy Policy shall state: "Please read our Privacy Policy notice." Overt warning signs or other graphics such as the

"skull and crossbones" or "cloak and dagger," or wording indicating danger or warning are specifically forbidden.

iv. The Martin Defense Group website will provide accessibility to all U.S. citizens, including persons with disabilities. This is not intended to permit open public access to those sites behind any security scheme, but those sites must be accessible to authorized persons who might also have disabilities.

e. Content of website

1. All information, graphics, and photos posted on publicly accessible the Martin Defense Group website must be carefully reviewed to ensure they meet the standards and requirements as published herein, including Operations Security (OPSEC) considerations.
2. Photos may not be altered in any way. Standard photographic practices of cropping, sizing, or burning are not considered an alteration.
3. The Martin Defense Group website shall:
    i. Be presented in a manner reflecting the professionalism of the Martin Defense Group.
    ii. Contain only "approved for release" general information suitable for viewing by anyone any place in the world, friend and foe alike.
    iii. Contain only those images which support the overall mission of the website. Images with captioning will only have caption information suitable for viewing by a worldwide audience, both internal and external. Images of personnel will not contain personal information other than name and position within the company.
4. Specific website restrictions include:
    i. The website shall not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. This includes, but is not limited to, lessons learned or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, etc., activities or information relating to ongoing criminal investigations into terrorist acts, force protection levels, specific force protection measures being taken or the number of personnel involved, Plans of the Day, or Plans of the Month are not permitted to be posted.
    ii. The website shall not identify family members of Martin Defense Group personnel in any way, including in photos or photo captions, except for the spouses of senior leaders who are participating in public events. Furthermore, family member information will not be included in any online biographies.
    iii. The website shall not contain any written information or display any logo indicating the website is best viewed with any specific web browser(s); or, that the website has been selected as a recommended or featured site by any organization; or, point to any particular search engines or recommend any

commercial software. Websites developed and/or maintained by contractors may not include the contractor's name nor may they link to the contractor's website.

iv. The website shall not provide commercial software or links to commercial software except in those cases where the software is unique and required for viewing documents provided within the Web site's purpose. An example is Adobe Acrobat required to read Portable Document Files (PDF) used for viewing documents that must be presented in an unalterable form. In these cases, only a text link directly to the vendors download web page is permitted. There will be no use of corporate logos.

v. The website shall not display any commercial page counters.

vi. The website shall not contain any material that is copyrighted or under trademark without the written permission of the copyright or trademark holder. The material must relate directly to Martin Defense Group's primary mission. Works prepared by Martin Defense Group personnel as part of their official duties and posted to the company website may not be copyrighted, nor may the website itself be copyrighted.

vii. The website shall not display personnel lists, "roster boards," organizational charts, or staff directories which show individuals' names, individuals' phone numbers or e-mail addresses which contain the individual's name.

viii. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable.

ix. The names, telephone numbers, and personalized, official e-mail addresses of public affairs personnel and/or those designated by management as the spokespersons may be included in otherwise non-personalized directories, etc.

x. Biographies of executive officers or management may be posted to the Martin Defense Group website. However, biographies published on the publicly accessible website will not include the date of birth, current residential location, nor any information about family members.

xi. Exceptions

1. Educational mission. In instances where the mission of the company includes an educational mission, and where unclassified dissertations or professional papers may be published to the Web for the purpose of peer review, the following disclaimer for exchange of professional information and ideas among scientists, engineers, or educators, must be displayed:

   "Material contained herein is made available for the purpose of peer review and discussion and does not necessarily reflect the views of the Martin Defense Group LLC or its clients or subcontractors."

2. Recruiting mission. Martin Defense Group may include advertising for employment opportunities.

f. Interactivity of website

1. Martin Defense Group may not operate unmoderated newsgroups, bulletin boards, or any other unrestricted access posting. This specifically prohibits a publicly accessible, services interactive site that supports automatic posting of information submitted by personnel other than those authorized by the company to post information. Some Weblogs (blogs) may fall into this category. This does not, however, prohibit the company from posting frequent messages from the executive team. There is also no prohibition on blogs operated by individual members as private citizens.
2. Public queries for information should be linked/directed to the site web manager or public affairs office. Queries should be handled consistent with other written requests for information. Responses shall discuss only those issues within Martin Defense Group's cognizance.

g. Collection of personal data

1. The Martin Defense Group website shall not collect any personal data (name, address, phone number, etc.) about a visitor. Network identification and Internet protocol addresses are not considered personal data.
2. The use of persistent cookies or any persistent identification element is prohibited on the website unless all of the following four conditions are met:
    i. The site provides clear and conspicuous notice of the use of cookies and a description of the safeguards for handling the information collected from the cookies.
    ii. There is a compelling need to gather the data on the site.
    iii. Appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies.
    iv. Web Bugs (i.e. tiny and/or invisible graphics on Web pages linked to third-party advertising, marketing, or eavesdropping entities or the like) and other automated means of collecting personally-identifying information without the express permission of the user are not included.

SOP #:	**MDG-AC-100**
Title:	**Account Management**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to manage information system accounts. This includes authorizing access, establishing and approving new accounts, setting and changing account privileges, and terminating accounts. Project Managers (PM) serve as Account managers.

2.0 Procedure

2.1 New Access

2.1.1 Folders in the Restricted network server

(1) Creating a new folder

(a) When a PM would like to create a new folder on the Restricted network server, the PM should email Martin Defense Group IT <it@mdefensegroup.com> with the following information:

(i) Folder and subfolder names (including a full pathway to such folder on the Restricted network server)
(ii) Full name list of all Users who should have access to (i) above
(iii) Type of access granted to Users in (ii) above: Read Only or Read/Write Access
(iv) Restrictions to Users in (ii) disallowing access to particular subfolders in (i) above
(v) The effective date of creation

(2) Granting access to an existing folder

(a) Project folders created by PMs

(i) When a PM would like to grant a User access to an existing folder on the Restricted network server, the PM should e-mail Martin Defense Group IT < it@mdefensegroup.com> asking to grant access to such User with the following information:

1. Full name of User
2. Folder name (including a full pathway to such folder on the Restricted network server)
3. Type of access: Read Only or Read/Write Access
4. Restrictions to the User in 1. disallowing access to particular subfolders in 2. Above, if any
5. Explanation of why the User needs access
6. The effective date of granting access

(b) Folders not created by PMs (e.g., Contracts, Proposals, etc.)

1. When a PM would like to grant a User access to an existing folder on the Restricted network server that he or she did not create, the PM

should e-mail the creator of such folder (e.g., Contracts Manager for the Contracts folder) asking for access and providing an explanation of why the User needs access.

2. Upon granting approval of such access, the creator of such folder should e-mail Martin Defense Group IT < it@mdefensegroup.com> asking to grant access to such User with the following information:

   a. Full name of User
   b. Folder name (including a full pathway to such folder on the Restricted network server)
   c. Type of access: Read Only or Read/Write Access
   d. Restrictions to User in a. disallowing access to particular subfolders in b. above, if any
   e. Explanation of why the User needs access
   f. The effective date of granting access
   g.

2.1.2 **Folders under the SharePoint platform through Microsoft Teams**

(1) Creating a new team

(a) When a PM would like to create a new team under Microsoft Teams, the PM should e-mail Martin Defense Group IT < it@mdefensegroup.com> with the following information:

(i) Team name
(ii) Full name list of all Users who should have access to (i) above
(iii) Type of access granted to Users in (ii) above: Read Only or Read/Write Access
(iv) The effective date of creation
(v) Project number xx-Kxxx or Department

(2) Granting access to an existing team

(a) When a PM would like to grant a User access to an existing team under Microsoft Teams, the PM can click the team name in Microsoft Teams at the top, click the "Add member" button, type the User name in the dialog box, click the Add button, and select either the "Owner" and "Member" role for the User.

2.2 **Modifying Privileges**

2.2.1 **Folders in the Restricted network server**

(1) Project folders created by PMs

(a) When a PM would like to modify access to an existing folder on the Restricted network server for a User, the PM should e-mail Martin Defense Group IT < it@mdefensegroup.com> asking to modify access to such User with the following information:

(i) Full name of User

(ii) Folder name (including a full pathway to such folder on the Restricted Drive)
(iii) Type of access: Read Only or Read/Write Access
(iv) Restrictions to Users in (i) disallowing access to particular subfolders in (ii) above, if any
(v) The effective date of modification

(2) Folders not created by PMs (e.g., Contracts, Proposals, etc.)

(a) When a PM would like to modify access to an existing folder on the Restricted network server for a User, the PM should e-mail the creator of such folder (e.g., Contracts Manager for the Contracts folder) asking for a modification of access.

(i) Upon granting approval of such modification, the creator of such folder should e-mail Martin Defense Group IT <It@mdefensegroup.com> asking to modify access to such User with the following information:

1. Full name of User
2. Folder name (including a full pathway to such folder on the Restricted network server)
3. Type of access: Read Only or Read/Write Access
4. Restrictions to Users in (1) disallowing access to particular subfolders in (3) above, if any
5. The effective date of modification

2.2.2 Folders under the SharePoint platform through Microsoft Teams

(1) When a PM would like to modify access to an existing team under Microsoft Teams for a User, the PM can click the team name in Microsoft Teams at the top and select either the "Owner" and "Member" role for the User under the list of members.

2.3 Terminating Access

2.3.1 Folders in the Restricted network server

(1) Project folders created by PMs

(a) When a PM would like to terminate access to an existing folder on the Restricted network server for a User, the PM should e-mail Martin Defense Group IT < it@mdefensegroup.com > asking to terminate access to such User with the following information:

(i) Full name of User
(ii) Folder name (including a full pathway to such folder on the Restricted network server)
(iii) The effective date of termination

(2) Folders not created by PMs (e.g., Contracts, Proposals, etc.)

(a) When a PM would like to terminate access to an existing folder on the Restricted network server for a User, the PM e-mail the creator of such folder

(e.g., Contracts Manager for the Contracts folder) asking for the termination of access.

(i) The creator of such folder should e-mail Martin Defense Group IT <It@mdefensegroup.com> asking to terminate access to such User with the following information:

1. Full name of User
2. Folder name (including a full pathway to such folder on the Restricted Drive)
3. The effective date of termination

2.3.2 **Folders under the SharePoint platform through Microsoft Teams**

(1) When a PM would like to terminate access to an existing team under Microsoft Teams for a User, the PM can click the team name in Microsoft Teams at the top and click the "X" box next to the User's name under the list of members.

2.4 **Review Access**

2.4.1 **Active Directory**. On a quarterly basis, the Audit Administrator shall review the Active Directory on to determine whether only Users who need access to folders in the Restricted network server are provided access (e.g., eliminate access for Users who are terminated or transferred away from a project from having access to the associated folder). The Audit Administrator shall also determine whether Users have the appropriate level of access as well as remove Users who no longer need access.

2.4.2 **SharePoint**. On a quarterly basis, the Audit Administrator shall review access to folders on the SharePoint platform to determine whether only Users who need access to such folders are provided access. The Audit Administrator shall also determine whether Users have the appropriate level of access as well as remove Users who no longer need access.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Responsible for maintaining user profiles in Active Directory to monitor User access. Creates, enables, modifies, disables, and removes information system accounts for Users.

3.1.2 PMs. Responsible for knowing which data on Martin Defense Group's information systems is CUI. Responsible for creating, enabling, modifying, disabling, and removing information system accounts for Users on the SharePoint platform.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	MDG-AC-101
Title:	Authenticator Management

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to manage information system account authenticator .

This includes initial authenticator establishment and distribution, distribution of multifactor authentication (MFA) tokens, changing authenticators, lost/compromised or damaged authenticators, and revoking authenticators.

2.0 Procedure

2.1 Initial Authenticator Establishment and Distribution

2.1.1 Designated IT Personnel shall create an initial authenticator (password) for new Users, which shall be randomly-generated letters and numbers. Initial authenticator distribution shall be accomplished either face to face or over the phone via voice or text.

2.1.2 Upon receipt of the initial authenticator, the User shall log in to the system and follow system prompts to immediately create a new password that complies with Martin Defense Group's password complexity policy (see Access Control Policy 4.2.a.7). Users shall not share their network password with anyone.

2.1.3 Designated IT Personnel shall then provide an MFA token to the User. When the User initially plugs in the MFA token, the MFA token software will prompt the User to establish a private PIN to use the token.

2.2 Lost/Compromised or Damaged Authenticators

2.2.1 Users promptly report loss, damage, or compromise of their authenticator or MFA token to Designated IT Personnel.

(1) Designated IT Personnel shall assist the User to recover/repair/replace the authenticator and notify the FSO of the incident.

(2) The Facility Security Officer shall initiate an investigation to determine if there are any potential reportable cybersecurity breaches.

3.0 Reference

3.1 Roles and Responsibilities

3.1.1 Designated IT Personnel.

(1) Establishes system parameters such that users are required to change their network password every 60 days. Establishes system parameters such that users must comply with Martin Defense Group's password complexity policy when changing passwords. Establishes system parameters that prohibit users from reusing passwords for a minimum of one (1) generation. Revokes authenticator(s) for users who no longer require access to Martin Defense Group's information system or have been inactive for more than 30 days.

(2) At the time of initial authenticator distribution for new user accounts, prepares an MFA token for use with Martin Defense Group's system and issues it to a User. Recovers MFA tokens from users who no longer require Martin Defense Group system access. Maintains an active inventory of all MFA tokens.

(3) Ensures that identifiers are never re-used.

(4) Configures information system to store and transmit only cryptographically protected passwords and obscure feedback of passwords when typed in.

3.2 **Definitions**. See Appendix C Glossary

SOP #:	MDG-AC-102
Title:	Information System Login

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to login to information system accounts. This includes logging in via direct (wired) access, wireless access, and restoring a network session.

2.0 Procedure

2.1 Direct (Wired) Access

2.1.1 Follow these steps to login to the information system via a wired connection:

(1) Ensure host (workstation or laptop, as applicable) is connected to the information system via Ethernet cable or similar; laptops may use a docking station for this purpose.
(2) Power-up host.
(3) Insert MFA smart card into card reader port on the computer (or docking station, as appropriate).
(4) When prompted, enter your username and password.

2.2 Wireless Access

2.2.1 Follow these steps to login to the information system via a wireless connection:

(1) Power-up host (workstation or laptop, as applicable).
(2) Insert MFA smart card into card reader on the computer (or docking station, as appropriate).
(3) When prompted, enter your username and password.
(4) Ensure Wi-Fi is enabled on the host.
(5) Connect to a Wi-Fi network.
(6) To also access the information on the Restricted network server, establish a VPN connection with the Fortinet VPN client (select “Corporate” under the WiFi screen and click the “Connect” button).

2.3 Restoring a Session

2.3.1 The information system is configured to prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from the user. To re-establish access from a session lock, follow these steps:

(1) Activate the login screen by simultaneously pressing the Ctrl, Alt, and Delete buttons.

(2) Insert MFA smart card into card reader on the computer (or docking station, as appropriate).

(3) When prompted, enter your username and password.

2.4 Unsuccessful Logins

2.4.1 After 5 consecutive login attempts, the session will be locked. Please wait 15 minutes before attempting to login again or contact the Designated IT Personnel.

3.0 Reference

3.1 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-AC-103**
Title:	**Use of Portable Storage Devices**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to manage the use of portable storage devices with the information system. This includes authorizing usage, inventory control, marking, encryption, physical protection, and disposal/release.

2.0 Procedure

2.1 **USB drive**: Users that wish to store information electronically (regardless of its classification as CUI or not) on a portable storage device may only do so using a USB drive issued by the IT department after sending a request to it@mdefensegroup.com. Users are prohibited from using all other devices such as portable hard drives or personal USB drives to store Martin Defense Group information.

2.2 **SD/micro SD/CF**: Users that wish to use recording devices such as a GoPro to conduct Martin Defense Group business may only do so using such a device issued by the IT department after submitting a request to it@mdefensegroup.com. Users are prohibited from using all other devices such as personal devices or company-issued cell phones to generate digital information for Martin Defense Group business.

2.2.1 Users are allowed to upload digital media from Martin Defense Group-issued devices to Martin Defense Group's network.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Must maintain an inventory of USB drives and recording devices issued to Users, which would include (1) make and model and (2) User name. Conducts annual audits of inventory to make sure such a device has not been lost or stolen. Designated office employees at remote offices will maintain and inventory of USB drives and recording devices at those specified locations.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-AC-104**
Title:	**Printing in a Network Environment**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to print documents containing CUI using printers connected to Martin Defense Group's information system.

2.0 Procedure

2.1 **Printing CUI**.

2.1.1 When printing documents containing or possibly containing CUI, an Information System User must choose a CUI Designated Printer in the software print screen and select "Secure Print" or "Private Print" in the Printer Properties rather than "Normal Print." The Information System User should then be prompted by the software to create a code.

2.1.2 The Information System User must then physically go to the selected CUI Designated Printer and input the code in step 2.1.1 above. This should release the hold on the print job, and the CUI Designed Printer will print the document.

2.2 **Verifying pages**. Upon picking up their document from the CUI Designated Printer, the Information System User should verify that they have picked up all of the pages of the document that was sent to such a printer.

2.3 **Dispose of CUI printouts**. If an Information System User decides not to keep any pages of a print job that contains CUI, they must dispose such pages according to the MP-102 Sanitizing Digital Media procedures.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Establishes system/network protocols to implement the procedures detailed herein. Determines which network printers may print documents containing CUI (Designated CUI Printers) by verifying whether a printer has secure print capabilities, which causes a print job to be placed on hold and not print until the Information System User inputs a code into the printer to release the hold. Places Designated CUI Printers in locations accessible only by a User. Notifies Information System Users which printers are Designated CUI Printers by placing labels on these printers stating that it is a "Designated CUI Printer."

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-AC-105**
Title:	**Publicly Accessible Content**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to protect Controlled Unclassified Information (CUI) from unauthorized disclosure via publicly-accessible systems.

2.0 Procedure

2.1 **Uploading content to the Martin Defense Group website**: A User who wishes to post content to the Martin Defense Group website must first send an e-mail to the FSO with a secure.mdefensegroup.com link to the content to request confirmation that such content does not contain CUI. Upon his or her approval after review, the Webmaster will upload the content to the appropriate online site, which will cause such content to appear on the Martin Defense Group website.

2.2 **Posting employment openings on the Martin Defense Group website:** A User who wishes to post an employment opening at Martin Defense Group must fill out a Job Requisition Form, prepare a Job Description for the position, and forward these two documents to the HR Manager. Upon his or her approval after review, the HR Manager will upload the Job Description to the appropriate online site, which will cause the employment opening to appear on the Martin Defense Group website.

2.3 **Annual website review**: The Audit Administrator will review Martin Defense Group's website on an annual basis to find any CUI in its content and immediately notify the Webmaster to remove any information verified by Users to be CUI.

2.4 Reference

2.4.1 **Definitions**. See Appendix C Glossary.

Assessment Policy

9 Overview

Properly auditing and assessing the organization, information system, and processes is a critical component of information security. Auditing prepares the system to identify inappropriate behaviors and provide clues to system attacks that have penetrated the information system boundaries. Assessments ensure that the processes and procedures are correct and effective. To that end, auditing and assessments of organization systems and processes, including but not limited to laptop computers, desktop computers, servers, and network devices, is to be managed according to rules set forth in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

10 Purpose

The purpose of this policy is to outline the required and acceptable methods for auditing and assessing information systems, policies, and procedures at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding auditing and assessments exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

11 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to use Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

12 Policy

12.1 Risk Assessment

Martin Defense Group:

a. Periodically assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. (3.11.1)[7]

[7] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

1. Conducts an assessment of risk, including the likelihood and magnitude of the harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; (RA-3a)
2. Documents risk assessment results in a risk assessment report;
3. Reviews and updates risk assessment results at least annually or when there are events or conditions that may impact the security of the system. (RA-3c, RA-3e)
4. Disseminates risk assessment results to system/network and audit administrators. (RA-3d)

b. Scans for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. (3.11.2)
   1. External scans are performed on a quarterly basis and when new vulnerabilities affecting those systems and applications are identified. (RA-5a)
   2. Internal scans are performed when the risk assessment is performed. (RA-5a)
   3. Analyzes vulnerability scan reports (RA-5c)
   4. Authorizes privileged access to system components for selected vulnerability scans.

c. Remediates vulnerabilities in accordance with assessments of risk. (3.11.3, RA-5d)

12.2 Security Assessment

Martin Defense Group:

a. Periodically assesses the security controls in organizational systems to determine if the controls are effective in their application. (3.12.1)
   1. Develops a security assessment plan that describes the scope of the assessment. (CA-2a)
   2. Assesses the security controls in the information system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; (CA-2b)
   3. Produces a security assessment report that documents the results of the assessment. (CA-2c)
   4. Analyzes results from security control assessments (RA-5c)

b. Develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. (3.12.2, CA-5a, CA-5b, CA-7f)

c. Monitors security controls on an ongoing basis to ensure the continued effectiveness of the controls. (3.12.3)
   1. Develops a continuous monitoring strategy document that drives the continuous monitoring program (CA-7)

2. Requires monthly monitoring reports and at least annual assessments supporting such monitoring that is provided to the Senior Management Official; (CA-7b, CA-7c, CA-7g)
3. Ongoing security status monitoring in accordance with the organizational continuous monitoring strategy (CA-7d)

d. Develops, documents, and periodically updates system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. (3.12.4, PL-2a.2, PL-2a.5, PL-2a.8, PL-2d)

1. Develops a security plan for the information system that is consistent with the organization's enterprise architecture. (PL-2a.1)
2. Describes the operational context of the information system in terms of missions and business processes. (PL-2a.3)

Configuration Management Policy

13 Overview

Properly managing organization information systems configurations is a critical component of information security. Properly configured systems reduce the potential for harming Martin Defense Group LLC (Martin Defense Group) through data theft, malware installation, and system damage. To that end, organization systems, including but not limited to laptop computers, desktop computers, servers, and network devices, is to be placed under configuration management according to rules set forth in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

14 Purpose

The purpose of this policy is to outline the required and acceptable methods for managing information systems configurations at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding configuration management exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

15 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to use Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

16 Policy

Martin Defense Group:

a. Establishes and maintains baseline configurations and inventory of organizational system components within the authorization boundary throughout the respective system development life cycles. (3.4.1, CM-8a.1, CM-8a.2, CM-8a.3, CM-8(1))[8]

    1. The baseline configuration documentation for each component includes: (CM-2)

        i. Operating system and its non-default configuration parameters;
        ii. Applications and their non-default configuration parameters;
        iii. Component installation and operation manuals;

[8] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

iv. Firmware documentation.

2. The inventory information includes: (CM-8a.4)

   i. Hardware - manufacturer, type, model, serial number, physical location;
   ii. Software – List of applications and the associated license information;
   iii. System component custodian;
   iv. Network information – name, IP address (if applicable), MAC address.

3. The baseline configuration and inventory are reviewed at least annually and when changes are made to the system to determine if changes/updates should be performed. (3.4.1, CM-8b)

b. Establishes and enforces security configuration settings for information technology products employed in organizational systems. (3.4.2, CM-6a)

c. Tracks, reviews, approves/disapproves, and audits changes to organizational systems. (3.4.3, CM-6c, CM-3b, CM-3c, CM-3d, CM-3e)

   1. The types of changes to the system that require CM control include; (CM-3a)

      i. Adding/removing a device
      ii. Modifying any security-related configuration of a perimeter, server, workstation, or network device.
      iii. Adding applications to any server or workstation
      iv. Modifying the network configuration of a workstation/server/network device
      v. Updating any software (operating system or application) of a workstation/server/network device

   2. A periodic review of the documented changes is performed every 30 days and a record of the review is captured (CM-3f)

d. Analyzes the security impact of changes prior to implementation. (3.4.4, CM-4)

e. Defines, documents, approves and enforces physical and logical access restrictions associated with changes to organizational systems. (3.4.5, CM-5)

f. Employs the principle of least functionality by configuring organizational systems to provide only essential capabilities. To that end, specific ports/protocols/services are disabled on all system components as listed in SOP MDG-CM-101. (3.4.6, CM-7a, CM-7b)

g. Restricts, disables, and prevents the use of nonessential programs, functions, ports, protocols, and services. (3.4.7, CM-7(2))

   1. Review every month what ports/protocols are available on the system, and if any ports/protocols are found that are not approved, then those ports/protocols are removed. (CM-7(1)a, CM-7(1)b)

   2. Execution of software applications are restricted to appropriate personnel and are operated within their license restrictions. (CM-7(2))

h. Applies deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy, as appropriate, to allow the execution of authorized software. (3.4.8, CM-7 (4)a, CM-7 (4)b, CM-7 (5)a, CM-7 (5)b)

1. Peer-to-peer file-sharing software applications specified in SOP MDG-CM-102 are not approved to operate on any organizational workstation/server. (CM-7(4)a)
2. All workstations are configured to prevent the execution of the peer-to-peer file-sharing software applications listed in SOP MDG-CM-102. (CM-7(4) b)
3. The software applications listed in SOP MDG-CM-100 are the only applications approved for use by the user role on Windows workstations. (CM-7(5)a)
4. All workstations are configured to only allow the user role to execute the applications listed in SOP MDG-CM-100. (CM-7(5) b)

i. Controls and monitors user-installed software. (3.4.9)

1. Software installation rights for workstations are reserved for Designated IT Personnel using active directory group policy. Software installation rights for servers are reserved for the system/network administrator role using active directory group policy. (CM-11a, CM-11b)
2. Workstation and server system components are configured to log the installation of software applications (CM-11c)

SOP #:	**MDG-CM-100**
Title:	**Authorized Applications**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the software applications authorized for use with Martin Defense Group information systems.

2.0 Procedure

2.1 **Authorized applications**. A list of authorized applications on Martin Defense Group's information systems is contained in a file managed by the IT department.

2.2 **Adding applications**. Users that wish to add applications not included in the list above to their computers must e-mail the IT department to have Designated IT Personnel to review, approve, and install such applications.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Responsible for conducting an annual review of the authorized applications.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-CM-101**
Title:	**Prohibited Ports/Protocols/Services**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify those ports, protocols, and services that are prohibited from use on Martin Defense Group's information systems.

2.0 Procedure

2.1 **Prohibited ports/protocols/services**. In compliance with our Configuration Management Policy, the following nonessential functions, ports, protocols, and services have been disabled from Martin Defense Group's information systems:

2.1.1 Web filter profile is set to block: Abortion, Advocacy Organizations, Alcohol, Alternative Beliefs, Dating, Gambling, Lingerie and Swimsuit, Marijuana, Nudity and Risque, Other Adult Materials, Pornography, Sex Education, Sports Hunting and War Games, Tobacco, Dynamic DNS, Malicious Websites, Phishing, and Spam URLs.

2.1.2 Web filter is set to warn for: Extremist Groups.

2.1.3 Services blocked: FastLemon.VPN, Hola.Unblocker, Hotspot.Shield, and Private.Internet.Access.VPN.

2.2 **Enabling ports/protocols/services**. Users that wish to enable any nonessential capability listed above on their computers must e-mail Martin Defense Group IT <it@mdefensegroup.com> to have Designated IT Personnel to enable such capability.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Responsible for:

(1) Reviewing what ports/protocols are available on Martin Defense Group's system every 6 months and remove any that are unapproved.

(2) Conducting an annual review of prohibited ports/protocols/services.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-CM-102**
Title:	**Prohibited Applications**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the software applications that are prohibited from use with Martin Defense Group information systems

2.0 Procedure

2.1 **Prohibited applications**. A list of prohibited applications on Martin Defense Group's information systems is managed by the IT department.

2.2 **Adding applications**. Users that wish to add any application included in the list above to their computers must e-mail the IT department to have specific applications reviewed and approved to install such applications.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Responsible for conducting an annual review of prohibited application

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-CM-103**
Title:	**Configuration Change Control**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to track, review, approve/disapprove, and audit changes to organizational systems.

2.0 Procedure

2.1 Designated IT Personnel must document changes to Martin Defense Group's organizational system (Configuration Documentation).

2.2 Designated IT Personnel shall review the Configuration Documentation every 30 days.

2.3 A notice will be provided to Users of upcoming changes. This will be identified at the weekly Friday IT status meeting.

3.0 Reference

3.1 **Definitions**. See Appendix C Glossary.

Media Protection and Backup Policy

17 Overview

Properly backing up organization information systems and protecting media are critical components of information security and reduce the potential for harming Martin Defense Group LLC (Martin Defense Group) through data theft, malware installation, and system damage. To that end, protection of media and backups of organization systems, including, but not limited to, laptop computers, desktop computers, servers, and network devices, are to be managed according to rules set forth in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

18 Purpose

The purpose of this policy is to outline the required and acceptable methods for protecting media and backing up information systems at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding media protection and backups exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

19 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to access Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

Policy

19.1 Media Protection

Martin Defense Group:

a. Protects (i.e., physically controls and securely stores) system media containing CUI (Controlled Unclassified Information), both paper and digital. (3.8.1, MP-4a, MP-4b)[9]

b. Limits access to CUI on system media to authorized users. (3.8.2, MP-2)

c. Adds into media that contain CUI.

d. Sanitizes or destroys system media containing CUI before disposal or release for reuse. (3.8.3, MP-6)

[9] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

e. Purge CUI from IT components before they are taken off-site for maintenance

f. Physical Removal and Sanitization of Information Systems [NIST MA-2(c) and NIST MA-2(d)]

g. Authorized personnel are to formally document any physical removal of information systems from facilities that are owned, operated, maintained, and/or controlled by Martin Defense Group. Approval procedures for physically removing information systems are to consist of the following: ISSM will be responsible for approving any physical removal of Information Systems and will log appropriate information pertaining to the removal, including reason for removal and any vendor related information. Additionally, all equipment is to be sanitized as necessary to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

h. Controls access to media containing CUI and maintains accountability for media during transport outside of controlled areas. (3.8.5, MP-5a, MP-5b)

i. Implements cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. (3.8.6, MP-5 (4))

j. Controls (restricts) the use of removable media on system components. USB removable drives are strictly controlled by Designated IT Personnel. (3.8.7, MP-7)

k. Prohibits the use of portable storage devices when such devices have no identifiable owner. (3.8.8, MP-7 (1))

l. Protects the confidentiality of backup CUI at storage locations. (3.8.9, CP-9d)

19.2 Backups

Martin Defense Group conducts backups of user-level information contained in the information system at least weekly. (CP-9a)

SOP #:	**MDG-MP-100**
Title:	**Media Marking Requirements**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to mark media with necessary Controlled Unclassified Information (CUI) markings and distribution limitations.

2.0 Procedure

2.1 **Distribution Statement Markings**: Media shall be marked in accordance with DoDM 5200.01 - Volume 4, which requires distributions statement markings based on Distribution Statement A – F classifications.

2.2 **Other Markings**: Any CUI not meeting the specific labeling instructions provided in DoDM 5200-01 Volume 4 shall have the following markings: (3.8.4, MP-3a). See the Martin Defense Group "Handling of Controlled Unclassified Information Manual" for more specifics to Martin Defense Group.

2.2.1 Electronic media shall contain one of the following notifications based on physical space available on the media:

(1) CUI… This media contains Controlled Unclassified Information and appropriate handling restrictions must be observed… CUI

(2) Controlled Unclassified Information

(3) CUI

2.2.2 All paper media shall be labeled with "Controlled Unclassified Information" on the front cover (if there is one), the title page, the first page, and the outside of the back cover (if there is one). Internal pages of the document that contain CUI shall be marked "CUI" at the bottom.

2.2.3

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 PMs. Responsible for determining the proper distribution statement markings for media.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-MP-101**
Title:	**Media Accountability**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to maintain accountability of media containing Controlled Unclassified Information (CUI) during transport outside of controlled areas.

2.0 Procedure

2.1 **Paper media**:

2.1.1 **Transport by mail**. If sent by mail, paper media containing or possibly containing CUI must be sent by U.S. Postal Service Registered, Express, or Certified Mail.

(1) The outer envelope must be marked "Do Not Forward. Return to Sender," and under no circumstances shall the USPS Express Mail label 11-B "Waiver of Signature and Indemnity" be used.

(2) The envelope must be taken to the post office, and the use of street mail collection boxes is prohibited.

(3) The paper media must be double-wrapped with opaque inner and outer covers. It shall be marked as follows:

(a) Mark the inner envelope top and bottom on both sides, preferably in red, with the classification in capital letters. A box, on the other hand, should be marked with the classification on all surfaces of the inner wrapping.

(b) Write the complete mailing address and complete return address on the inner envelope. The address on the inner envelope should have the name of an appropriately cleared individual.

(c) On the outer envelope, write the complete mailing address and return address. Do not indicate on the outer envelope that it contains classified information. The mail or shipment should be addressed to the recipient by title, not by name, or to an approved classified mailing address of a federal activity or to a cleared contractor using the name and classified mailing address of the facility. An individual's name should not appear on the outer envelope. Instead of a person's name, use office code letters, numbers, or phrases in an attention line to aid in internal routing. When necessary to direct material to the attention of a particular individual, put the individual's name on an attention line in the letter of transmittal or on the inner container or wrapper.

(4) A receipt identifying the sender, the addressee, and the document should be attached to or enclosed in the inner envelope if the sender deems necessary or if the information is being sent to a foreign government.

2.1.2 **Transport by foot or car**. If transported by foot or car, paper media containing or possibly containing CUI must be double wrapped or packaged as though it were being sent by mail, kept under the User’s constant control (i.e., not left in the trunk of the car while the User runs another errand), and delivered only to an authorized

person. A briefcase may serve as the outer wrapper only if it is locked and approved for carrying such material by the FSO. Prepare an inventory of the material and leave one copy in the User's office and another copy with the FSO. Carrying CUI on trips that involve an overnight stopover is not permitted without advance arrangements for overnight storage in a U.S. Government office or a cleared contractor facility.

2.1.3 **Transport by air travel**. If transported by air travel, paper media containing or possibly containing CUI may only be transported by a User after obtaining a written letter of authorization from the FSO.

2.2 **Electronic media**:

2.2.1 **CUI stored on a physical device:** CUI may only be stored on a burned CD/DVD, Martin Defense Group-issued laptop, or Martin Defense Group-owned USB drive and must be kept under constant control by the User.

(1) If sent to a destination by mail, transported by foot or car, or transported by air travel, the electronic media must be treated as paper media and satisfy all of the requirements in paragraph 2.1.1, 2.1.2, or 2.1.3, respectively. For purposes of double wrapping, the media device does not count as inner wrapping.

2.2.2 **CUI transported electronically**:

(1) **Email**: CUI may not reside inside the body of or as an attachment to e-mails. When e-mailing others, Users may only provide access to CUI as Liquidfiles links.

(2) **Website upload or other file transmission methods**: CUI must be encrypted with FIPS 140-2 level encryption before transmission to others through means other than e-mail.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel. Ensures that company-issued phones and laptops are encrypted and key vaulting is implemented.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-MP-102**
Title:	**Sanitizing Digital Media**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to sanitize or destroy system media containing Controlled Unclassified Information (CUI) before disposal or release for reuse.

2.0 Procedure

2.1 **Paper media**: Users must place unwanted documents containing or possibly containing CUI into shred bins provided by Martin Defense Group.

2.2 **CD/DVDs**: Users must place unwanted CD/DVDs containing or possibly containing CUI into shred bins provided by Martin Defense Group.

2.3 **Laptops and workstations**: Users must return unused laptops and workstations to Designated IT Personnel for sanitation.

2.4 **Martin Defense Group-issued USB drives**: Users must return unused Martin Defense Group USB drives to Designated IT Personnel for sanitation.

2.5 **SD/micro SD/CF cards in Martin Defense Group-issued devices**: Users must return unused Martin Defense Group-issued devices containing SD/micro SD/CF cards to Designated IT Personnel for sanitation.

Reference

2.6 **Roles and Responsibilities**

2.6.1 Designated IT Personnel: Responsible for sanitizing laptops, workstations, Martin Defense Group-issued USBs, and SD/micro SD/CF cards in compliance with DoD 5220.22-M procedures.

2.6.2 FSO and/or Office Manager: Responsible for placing shred bins that comply with DoD 5220.22-M procedures in each Martin Defense Group branch.

3.0 Reference

3.1 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-MP-103**
Title:	**Backups of User-Level Information**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to ensure the availability of the data in Martin Defense Group's information systems by protecting it from inadvertent loss due to system/hardware failures or natural disasters.

2.0 Procedure

2.1 **Encryption for backups**. For purposes of backing up server information, Designated IT Personnel must use software (currently Veeam) and storage (currently AWS GovCloud) that encrypts data during transit and rest.

2.2 **Periodic backups**. Designated IT Personnel shall conduct backups of user-level information at least weekly.

3.0 Reference

3.1 **Definitions**. See Appendix C Glossary.

Monitoring and Systems/Communications Protection Policy

20 Overview

Properly monitoring and protecting Martin Defense Group's information and communications systems and the activities within them are critical components of information security. Protecting information and communications systems helps prevent inappropriate behaviors and provide clues to system attacks that have penetrated the information system boundaries. To that end, the monitoring and protection of organization systems and communications, including but not limited to laptop computers, desktop computers, servers, and network devices, is to be managed according to rules set forth in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

21 Purpose

The purpose of this policy is to outline the required and acceptable methods for monitoring and protecting the information and communications systems at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding these protections exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

22 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to use Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

23 Policy

23.1 Audit and Accountability

Martin Defense Group:

a. Creates, protects, and retains system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Determines that the information system is capable of auditing the events

specified in SOP MDG-MSP-100. (3.3.1, AU-2a, AU-2d, AU-12a)[10]

b. Ensures that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. (3.3.2, AU-3)

c. Reviews and updates the audited events list at least annually. (3.3.3, AU-2(3))

d. Alerts system/network and audit administrators in the event of an audit process failure. (3.3.4, AU-5a)

e. Correlates audit reviews, analyses, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. (3.3.5).

    1. Reviews and analyzes information system audit records continuously for indications of inappropriate or unusual activity; (AU-6a)

    2. Reports findings to the Incident Response Team. (AU-6b)

    3. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. (AU-6(3))

f. Provides an audit reduction and report generation capability within the information system that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. (3.3.6, AU-7a)

g. It provides a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. (3.3.7)

    1. The information system uses internal system clocks to generate timestamps for audit records (AU-8a)

    2. The information system compares the internal information system clocks at least every 24 hours with NIST authoritative time source (AU-8(1)a)

h. Using the information system protects audit information and audit tools from unauthorized access, modification, and deletion. (3.3.8, AU-9)

i. Limits management of audit functionality to a subset of privileged users, specifically audit administrators only. (3.3.9, AU-9(4))

23.2 System and Communications Protection

a. Martin Defense Group:

    1. Employs architectural designs, software development techniques, and system security engineering principles in the specification, design, development, implementation, and modification of the information system that promotes effective information security within organizational systems. (3.13.2, SA-8)

[10] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

2. Establishes and manages cryptographic keys for required cryptography employed in organizational systems per NIST FIPS-compliance. (3.13.10, SC-12)
3. Cryptographic Key Establishment and Management & Protection [NIST SC-12, NIST SC-13] Martin Defense Group LLC establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with mandated requirements, and that encryption is used where necessary for ensuring information is protected during transit, and at rest. Martin Defense Group LLC will abide by the recommendations for key management established in NIST SP 800-57 Parts 1 – 3, DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling", DoDI 8520.03 "Identity Authentication for Information Systems.", and NSA Key Management Requirements Annex v1.0. Martin Defense Group LLC produces, controls, and distributes cryptographic keys using NSA-approved key management technology and processes. Martin Defense Group LLC's initiatives related to cryptographic key establishment and management are listed in the matrix below:

Cryptography/Encryption Used	Description of Cryptographic Key Measures Used
Data at Rest	All data is encrypted using Microsoft Bitlocker on all hard drives. All Bitlocker recovery keys are printed and stored in the safe.
Data in Transit	All NFS traffic is encrypted in transit using Transport Layer Security (TLS) 1.2. The system is configured to use FIPS-compliant algorithms for encryption, hashing, and signing.
Storage	Cryptographic keys are all stored in the Windows Certificate Store on each computer and backed up during normal maintenance windows.
Access	The organization maintains availability of information in the event of the loss of cryptographic keys by users. All users have access to the Windows Certificate Store.
Destruction	When there are no further requirements for retaining KM or its association with an entity, the key will be de-registered (i.e., all records of the KM and its associations should be destroyed), and all copies of the private or secret key will be destroyed. Any media on which the KM was stored will be erased in a manner that removes all traces of the KM so that it cannot be recovered by either physical or electronic means.

4. Controls and monitors the use of mobile code within the information system. (3.13.13, SC-18c)
    i. Logged mobile code includes ActiveX, Shockwave, JavaScript, VBA script, and Java applet.
    ii. Denied mobile code includes: Flash
    iii. Utilizing PDF files with approved readers.
5. Martin Defense Group shall implement a tamper protection program for the information system, system component, or information system service to protect the network from mobile code that performs unauthorized and malicious actions. The following are categories of mobile code/active content:
    i. Category 1/high risk mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, server and remote system services and resources. These pose a significant risk to the company's information systems because they allow unlimited access to a user's computer. There are two subgroups of Category 1 mobile code technologies:
    ii. Category 1 technologies can differentiate between signed and unsigned mobile code. The technologies can also be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. Category 1 mobile code technologies may be used by Martin Defense Group when additional restrictions are implemented. The following are assigned to Category 1:
        (a) ActiveX controls
        (b) Shockwave movies (e.g., dcr, .dxr, .dir files), including Xtras, that execute in the Shockwave for Director plug-in.
    iii. Category 1 consists of mobile code technologies that are prohibited from use on information systems beyond the local information system's authorization boundary, or to or from external entities because they cannot differentiate between signed and unsigned mobile code nor can they be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code. The following are assigned to Category 1:
        (a) Mobile code scripts that execute in Windows Scripting Host (WSH) (e.g., JavaScript or VBScript downloaded via URL file reference or email attachments)
        (b) Hypertext Mark-up Language (HTML) applications (e.g., .hta files) that download as mobile code • Scrap objects (e.g., .shs and .shb files)
        (c) Microsoft Disk Operating System (MS-DOS) batch scripts
        (d) UNIX shell scripts
        (e) Binary executables (e.g., .exe files) that download as mobile code
    iv. Category 1 mobile code must be obtained from a trusted source and must be signed with a company approved PKI code-signing certificate.

v. iii. All information systems capable of executing mobile code must be configured to disable the execution of unsigned Category 1 mobile code obtained from outside the managed boundary.
vi. Category 2/medium risk mobile code technologies have full functionality, allowing mediated or controlled access to workstations, server, and remote system services and resources. Category 2 technologies can pose a moderate security threat to the information systems because they offer limited control by the user on what the code is allowed to do. They may be used when the Category 2 restrictions are implemented.
vii. The following are assigned to Category 2:
    (a) Java applets and other Java mobile code
    (b) Visual Basic for Applications (VBA) (e.g., Microsoft Office macros)
    (c) LotusScript (e.g., Lotus Notes scripts)
    (d) PerfectScript (e.g., Corel Office macros)
    (e) Postscript
    (f) Mobile code executing in .NET Common Language Runtime
viii. Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel (i.e., TLS VPN, IPsec, or other approved by the ESRMO).
ix. Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, or network connections other than to its originating host).
x. Where technically configurable, web browsers and other mobile code-enabled products must be configured to prompt the user prior to the execution of Category 2 code.
xi. Where technically configurable, protections against malicious Category 2 technologies must be employed at end user systems and at system boundaries.
xii. Category 3/low risk mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 mobile code may be freely used without restrictions in information systems. Category 3 technologies pose limited risk to the information systems because they are very restricted in the actions they can perform. The following are assigned to Category 3:
    (a) JavaScript, including Jscript and European Computer Manufacturers Association (ECMA) Script variants, when executing in the browser
    (b) VBScript, when executing in the browser
    (c) Portable Document Format (PDF)
    (d) Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash plug-in

xiii. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and therefore have not been assigned to one of the three risk categories described above. Emerging mobile code technologies must not be used unless approved by the IT department. The download and execution of mobile code using emerging technologies must be blocked by all means available at the network boundary, workstation, host, and within applications.

6. Controls and monitors the use of Voice over Internet Protocol (VoIP) technologies within the information system, separating VOIP systems into a separate VLAN from systems handling CUI. (3.13.14, SC-19b)

b. The information system:

1. Monitors, controls, and protects communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. (3.13.1)
    i. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system (SC-7a)
    ii. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. (SC-7c)
2. Separates user functionality (including user interface services) from information system management functionality. (3.13.3, SC-2)
3. Prevents unauthorized and unintended information transfer via shared system resources. Only modern operating systems that support object reuse requirements may be used for workstation and server components. (3.13.4, SC-4)
4. Implement subnetworks for publicly-accessible system components that are physically or logically separated from internal organizational networks. (3.13.5, SC-7b)
5. Denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). (3.13.6, SC-7 (5))
6. Prevents remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. (3.13.7, SC-7 (7))
7. Implements cryptographic mechanisms to prevent unauthorized disclosure of Controlled Unclassified Information (CUI) during transmission unless otherwise protected by alternative physical safeguards. (3.13.8)
    i. The information system protects the confidentiality of transmitted information. (SC-8)

ii. The information system implements cryptographic mechanisms to prevent unauthorized disclosure of sensitive information during transmission unless otherwise protected by alternative physical safeguards when traversing areas not approved for the sensitivity of the information. (SC-8 (1))

8. Employs FIPS-validated cryptography when used to protect the confidentiality of CUI in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. (3.13.11, SC-13)
9. Terminates network connections associated with communications sessions at the end of the sessions or after 15 minutes of inactivity. (3.13.9, SC-10)
10. Prohibits remote activation of collaborative computing devices and provides an indication of devices in use to users present at the device. (3.13.12)
    i. Prohibits remote activation of collaborative computing devices with the following exceptions: dedicated VTC suites, which rely on one of the participants calling or connecting to the other party to activate the video conference, located in approved VTC locations that are centrally managed. (SC-15a)
    ii. It provides an explicit indication of use to users physically present at the devices. Where such an indicator is not feasible, provides a means to physically obstruct the device. (SC-15b)
11. Protects the authenticity of communications sessions. (3.13.15, SC-23)
12. Protects the confidentiality of CUI at rest. (3.13.16, SC-28)

23.3 System and Information Integrity

Martin Defense Group:

a. Identifies, reports and corrects information system flaws in a timely manner. (3.14.1)
    1. Identifies, reports, and corrects information system flaws (SI-2a)
    2. Installs security-relevant software and firmware updates within 30 days of the release of the updates (SI-2c)
b. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. (3.14.2, SI-3a)
c. Monitors system security alerts and advisories and takes appropriate actions in response. (3.14.3)
    1. Receives information system security alerts, advisories, and directives from the US-CERT on an ongoing basis. (SI-5a)
    2. Generates internal security alerts, advisories, and directives as deemed necessary (SI-5b)
    3. Disseminates security alerts, advisories, and directives to system/network and audit administrators. (SI-5c)

4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance (SI-5d)

d. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. (3.14.4, SI-3b)

e. Performs periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed. (3.14.5)

    1. Configures malicious code protection mechanisms to perform periodic scans of the information system at least weekly and real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy (SI-3c.1)
    2. Configures malicious code protection mechanisms to block and quarantine malicious code then send an audit event in response to malicious code detection (SI-3c.2)

f. Continuously monitors organizational systems, including inbound and outbound communications traffic, for unusual or unauthorized activities or conditions to detect attacks and indicators of potential attacks. (3.14.6, SI-4(4))

g. Identifies unauthorized use of organizational systems. (3.14.7)

    1. Monitors the information system to detect attacks and indicators of potential attacks with the objective of preventing incursions and, when they occur, to reduce the time that an incursion is active. (SI-4a.1)
    2. Monitors the information system to detect unauthorized local, network, and remote connections. (SI-4a.2)
    3. Identifies unauthorized use of the information system through monitoring communications and system logs. (SI-4b)
    4. Deploys monitoring devices:
        i. Strategically within the information system to collect organization-determined essential information; (SI-4c.1) and
        ii. At ad hoc locations within the system to track specific types of transactions of interest to the organization. (SI-4c.2)
    5. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. (SI-4d)
    6. Provides system monitoring and log information to system/network and audit administrators as needed. (SI-4g)

SOP #:	**MDG-MSP-100**
Title:	**System Audit Events**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the system events that require auditing.

2.0 Procedure

2.1 **System audits**. Designated IT Personnel shall install the software (currently Forticlient) on Martin Defense Group's information systems to monitor the network and generate audit records. Designated IT Personnel shall ensure that the software generates audit records are sufficient to trace actions to specific Users and time stamps the record with time.nist.gov.

2.1.1 Trusted Internet LLC, a third party hired by Martin Defense Group, shall review the audit records generated by Forticlient, provide monthly reports to Martin Defense Group organizing this data, and notify Martin Defense Group of audit process failures and indications of inappropriate, suspicious, or unusual activity. Trusted Internet shall also provide Martin Defense Group with network audit logs generated by Martin Defense Group's firewall software, which Trusted Internet manages.

2.1.2 Designated IT Personnel shall analyze Trusted Internet's reports and network audit logs and the Microsoft GCC High data on a monthly basis to correlate them to detect any inappropriate, suspicious, or unusual activity.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 Designated IT Personnel and Audit Administrator. Shall have sole access to audit records and logs generated by Trusted Internet.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	MDG-MSP-101
Title:	Collaborative Computing Devices

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to protect organizational information, including Controlled Unclassified Information (CUI), by preventing unauthorized personnel from participating in collaborative computing sessions.

2.0 Procedure

2.1 Conducting teleconferences

2.1.1 Users may only access Martin Defense Group video cameras using approved video conference software, such as Microsoft Teams, on Martin Defense Group-issued equipment to conduct teleconferences for Martin Defense Group-related business. Users may not access Martin Defense Group video cameras remotely from non-Martin Defense Group issued equipment.

2.1.2 Users may not use non-Martin Defense Group issued equipment (e.g., personal video cameras) to conduct any Martin Defense Group-related teleconferences.

3.0 Reference

3.1 Roles and Responsibilities

3.1.1 Designated IT Personnel. Must purchase video cameras of a uniform brand and model for installation in all sites that allow for teleconferences (both onsite and offsite Martin Defense Group premises if any). These devices must provide an indication (e.g., light turn on) when they are actively transmitting data. Must ensure that non-Martin Defense Group issued equipment cannot access Martin Defense Group video cameras.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	MDG-MSP-102
Title:	System and Information Integrity

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to identify and eliminate potential information system security vulnerabilities.

2.0 Procedure

2.1 Access Control

2.1.1 Account Management

(1) **User accounts**. Designated IT Personnel shall only assign user accounts to Users and shall not provide administrative accounts to Users.

(2) **Administrator accounts**. Designated IT Personnel shall have a separate (1) user account to conduct user functions and (2) administrator account to conduct administrative functions. Designated IT Personnel may not conduct user functions on his or her administrative account.

(3) **Active Directory**. Using Active Directory, Designated IT Personnel shall prevent Users from accessing any information in the Restricted network server unless the User is granted access through the AC-100 Account Management procedures.

(4) **SharePoint access**. PMs shall prevent Users from accessing any information on the SharePoint platform unless the User is granted access through the AC-100 Account Management procedures.

(5) **Login banner**. Designated IT Personnel shall configure all systems to display a banner to users before granting access to the system that provides privacy and security notices consistent with applicable CUI laws.

2.1.2 Automatic Session Terminations

(1) Designated IT Personnel shall configure systems to automatically terminate after the following periods of inactivity:
(a) Remote Desktop Protocol (RDP) sessions: 15 minutes.
(b) Secure Shell (SSH) sessions: 15 minutes.

2.1.3 Remote Access

(1) Using remote access, Designated IT Personnel may perform limited number of privileged commands including system account management, firewall/VPN configuration, and log archiving.

(2) Using remove access, Designated IT Personnel may access limited security related information including user account information, firewall configuration data, and log files.

2.1.4 Mobile Devices

(1) Designated IT Personnel shall prevent any mobile device other than company-issued laptops, notebooks, and cellphones from connecting to Martin Defense Group's network.

2.1.5 **External Systems**

(1) Designated IT Personnel shall prohibit the use of all file sharing services except for the following:
(a) Microsoft OneDrive
(2) secure.mdefensegroup.com. Only when necessary to share information with external users.

2.1.6 **Publicly Accessible Content**

(1) **Website**. Designated IT Personnel shall host Martin Defense Group's website on a web server (currently GoDaddy) that is physically separate from Martin Defense Group's network.

2.1.7 **Screening**

(1) Martin Defense Group's Human Resources Manager shall conduct the following background checks before employees are authorized access to CUI: drug/alcohol, nationwide criminal background check, and citizenship verification.

2.2 **Assessment**

2.2.1 **Risk Assessment**

(1) Trusted Internet, Inc., an outside vendor hired by Martin Defense Group, shall perform an initial assessment of risk to Martin Defense Group's information system, generate monthly monitoring reports, and update the assessment on an annual basis. Trusted Internet shall provide the risk assessment results to the System/Network Administrator and the Audit Administrator.

(2) Based on the risk assessment, Designated IT Personnel shall use host software (currently FortiClient) to apply appropriate software patches to eliminate vulnerabilities.

(a) For those vulnerabilities that cannot be resolved using software patches, Designated IT Personnel shall develop a plan of action to resolve the issue within two weeks from the development date of this plan.

2.2.2 **Security Assessment**. Designated IT Personnel shall do a full assessment of all of Martin Defense Group's security controls and then do an annual assessment of all critical controls and 1/3 of the remaining controls.

2.2.3 **Vulnerabilities**. Designated IT Personnel shall configure vulnerability scanner software (currently Nessus) to scan for vulnerabilities in Martin Defense Group's network on a quarterly basis. Upon completion of each scan, Designated IT Personnel shall analyze the vulnerability scan report and fix such vulnerabilities.

2.2.4 **System Security Plan (SSP)**.

(1) The System/Network Administrator shall develop a SSP that describes system boundaries, system environments of operation, how security requirements are

implemented, and the relationships with or connections to other systems and update this plan on an annual basis.

(2) Designated IT Personnel and the FSO shall update the SSP on an annual basis.

2.3 **Media Protection and Backup**

2.3.1 **Encryption**. Designated IT Personnel shall encrypt all of Martin Defense Group's network servers, laptops, workstations, and backups with FIPS 140-2 level encryption (currently using BitLocker software). Designated IT Personnel shall collect and manage all cryptographic keys through a spreadsheet.

2.4 **Monitoring & Systems/Communications Protection**

2.4.1 **Network traffic**. Designated IT Personnel shall configure network software (currently FortiGate) to deny network traffic by default with exceptions made for authorized programs.

2.4.2 **Split tunneling**. Designated IT Personnel shall configure software (currently FortiGate Virtual Private Network) to prevent split tunneling into Martin Defense Group's network.

2.4.3 **System flaws**. Designated IT Personnel shall configure software (currently Forticlient) to identify system flaws on Martin Defense Group's network. Designated IT Personnel shall configure software (currently Windows Server Update Services) to update any system flaws discovered in a timely manner.

2.4.4 **Malicious Code Protection**

(1) Designated IT Personnel shall configure boundary intrusion prevention systems, antivirus, and firewall software (currently FortiGate) to provide protection against malicious code from external sources as well as host-based antivirus software (currently FortiClient) on all Martin Defense Group laptops and workstations.

(2) Designated IT Personnel shall configure software (currently Microsoft Office 365 Advanced Threat Protection) to scan e-mail attachments for malware and viruses.

(3) Designated IT Personnel shall configure software to perform weekly antivirus scans and have real time protection enabled.

2.4.5 **Security alerts**. The System/Network Administrator and Audit Administrator shall register with the United States Computer Emergency Readiness Team and Defense Industrial Base Cybersecurity Program to receive security alerts and advisories.

2.4.6 **Communications traffic**. Designated IT Personnel shall configure firewall software (currently FortiGate) to monitor inbound and outbound communications traffic.

2.4.7 **Unauthorized use**. Designated IT Personnel shall configure software (currently Forticlient) to identify unauthorized use of Martin Defense Group's network.

2.4.8 **Mobile code**. Designated IT Personnel shall log mobile code including ActiveX, Shockwave, JavaScript, VBA script, and Java applet and deny the use of Flash.

3.0 Reference

3.1 **Definitions**. See Appendix C Glossary.

Personnel Security Policy

24 Overview

Properly maintaining personnel security is a critical component of information security. Maintaining personnel security reduces the potential for harming Martin Defense Group LLC (Martin Defense Group) through data theft, malware installation, and system damage. To that end, personnel security is to be managed according to rules set forth in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

25 Purpose

The purpose of this policy is to outline the required and acceptable methods for maintaining personnel security at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding personnel security exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

26 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to access Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

27 Policy

Martin Defense Group:

a. Screens individuals prior to authorizing access to organizational systems containing CUI. Such screening shall consist of the following: drug/alcohol, nationwide criminal background check, and citizenship verification. (3.9.1, PS-3a)[11]

b. Ensures that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. (3.9.2)

    1. Upon termination of individual employment:

[11] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

i. Disables information system access within no more than five (5) working days after the final day of employment if the termination is voluntary, or within the same day if the termination is involuntary; (PS-4a)

ii. Terminates/revokes any authenticators/credentials associated with the individual; (PS-4b)

iii. Conducts exit interviews that include a discussion of CUI protection requirements; (PS-4c)

iv. Retrieves all security-related organizational information system-related property; (PS-4d)

v. Retains access to organizational information and information systems formerly controlled by terminated individual; and (PS-4e)

vi. Notifies the system/network administrator as soon as possible, not to exceed one (1) working day. (PS-4f)

2. Upon transfer of personnel:

i. Reviews and confirms the ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. (PS-5a)

ii. Initiates reassignment actions to ensure all system access that is no longer required (need to know) is removed or disabled within 10 working days. (PS-5b)

iii. Modifies access authorization as needed to correspond with any changes in operational needs due to reassignment or transfer. (PS-5c)

iv. Notifies system/network administrator as soon as possible, not to exceed 1 working day. (PS-5d)

SOP #:	**MDG-PS-100**
Title:	**Transfers and Terminations**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to ensure that Controlled Unclassified Information (CUI) and organizational systems containing CUI are protected during and after personnel actions such as transfers and terminations.

2.0 Procedure

2.1 Transfer of Personnel

2.1.1 Upon notification by the HR Manager or a PM that a User is transferring (not to exceed one working day), Designated IT Personnel shall review and update the User's Active Directory profile to reflect changes in a User's role within 10 working days.

2.1.2 Within 10 working days of notification of a User's transfer, PMs shall review the User's access to folders on the Restricted network and under the SharePoint platform and follow the Terminating Access procedures outlined in the Account Management procedures to remove access that the User no longer needs.

2.2 Termination of Employment

2.2.1 Upon notification by the HR Manager or a PM that a User's employment with Martin Defense Group is terminating (not to exceed one working day), Designated IT Personnel must determine whether the termination is voluntary or involuntary and disable the User's ability to login to Microsoft 365, Active Directory, and all cloud-based applications on the appropriate effective date.

(a) For voluntary terminations, the effective termination date is the day after the User's planned departure date.
(b) For involuntary terminations, the effective termination date is the middle of the day on which the User will be notified of his/her termination.

2.2.2 The HR Manager must collect all Martin Defense Group-issued equipment (e.g., laptops, Martin Defense Group-issued USBs, Martin Defense Group-issued GoPros, etc.) (1) by the end of the User's planned departure date for voluntary terminations or (2) upon notification of the termination to the User for involuntary terminations. The HR Manager must also include a discussion of CUI protection requirements in the exit interview with the User.

3.0 Reference

3.1 Roles and Responsibilities

3.1.1 Designated IT Personnel. Take the following actions within no more than five (5) working days after the final day of employment if termination is voluntary, or within the same day if termination is involuntary. Indicate completion of these actions by checking the appropriate block:

– Disable the account's information system access.

- Revoke account authenticators/credentials.
- Retain access to the account's organizational information.

3.2 **Definitions**. See Appendix C Glossary.

Physical Security Policy

28 Overview

Properly managing organization physical security is a critical component of information security. Proper physical security reduces the potential for harming Martin Defense Group LLC (Martin Defense Group) through data theft, malware installation, and system damage. To that end, organization facilities, including but not limited to Martin Defense Group physical spaces and other spaces used for accessing Martin Defense Group systems or data, are to be physically secured according to rules outlined in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

29 Purpose

The purpose of this policy is to outline the required and acceptable methods for managing the physical security of information systems at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding physical security controls exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

30 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to use Martin Defense Group computers and systems following Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

31 Policy

Martin Defense Group:

a. Limits physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. (3.10.1)[12]

    1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. (PE-2a)
    2. Issues authorization credentials for facility access. (PE-2b)

[12] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

3. Reviews the access list detailing authorized facility access by individuals at least semi-annually. (PE-2c)
4. Removes individuals from the facility access list when access is no longer required. (PE-2d)
5. Access to the CUI area by individuals is only provided if they are on the authorized access list or they are escorted by authorized personnel. (PE-3a1)

b. Protects and monitors the physical facility and support infrastructure for organizational systems. (3.10.2)
    1. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output. (PE-5)
    2. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents. (PE-6a)
    3. Review physical access logs at least every 90 days and upon the occurrence of a physical access incident. (PE-6b)
    4. Coordinate results of reviews and investigations with the organizational incident response capability. (PE-6c)
c. Escorts visitors and monitors visitor activity in all circumstances within restricted access areas where the information system resides. (3.10.3, PE-3d)
d. Maintains physical access audit logs for all entry/exit points. (3.10.4, PE-3b)
e. Controls and manages physical access devices. (3.10.5)
    1. Spare physical keys and copies of combinations are stored in a locked container. (PE-3e)
    2. Inventories physical keys at least annually. (PE-3f)
    3. Changes combinations and keys when keys are lost, combinations are compromised, an individual has shared his or her password, or individuals are transferred or terminated. (PE-3g)
f. Imposes a clean desk policy.
    1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
    2. Computer workstations must be locked when the workspace is unoccupied.
    3. Computer workstations must be shut down completely at the end of the workday.
    4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
    5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when unattended.
    6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

7. Laptops must be either locked with a locking cable or locked away in a drawer.
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
10. Upon disposal, Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Restricted and/or Sensitive information should be erased.
12. Lock away portable computing devices such as laptops and tablets.
13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
14. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

g. Enforces safeguarding measures for CUI at alternate worksites (e.g., telework sites, satellite offices) by employing appropriate NIST 800-171 based security requirements. (3.10.6, PE-17a). Follow guidelines as documented in https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final

h. Provides a means for Users to communicate with information security personnel in case of security incidents or problems. (PE-17c)

SOP #:	MDG-PHYS-100
Title:	Authorized Access

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to protect the physical security of Martin Defense Group's information systems.

2.0 Procedure

2.1 Access to Martin Defense Group Premises

2.1.1 **Door locks**. To ensure that only Authorized Users have access to Martin Defense Group's work area premises, the FSO and/or Office Manager shall install locks on all Martin Defense Group doors and issue Users access cards and/or keys to unlock them and badges that contain their picture and employee id #.

(1) User access cards and/or keys must not be shared or loaned to others.

(2) All access cards and/or keys that are no longer required must be returned to the FSO and/or Office Manager.

(3) Lost or stolen cards and/or keys must be reported immediately to the FSO and/or Office Manager.

(4) The FSO and/or Office Manager shall remove the card and/or key access rights of Users that change roles or are separated from Martin Defense Group.

(5) The FSO and/or Office Manager shall develop and maintain a list of individuals with access cards and/or keys to Martin Defense Group's facilities (Access List).

(6) The FSO and/or Office Manager shall review the Access List at least semi-annually.

(7) The FSO and/or Office Manager shall review physical access logs generated by the software for Martin Defense Group's doors at least every 90 days and upon the occurrence of a physical access incident.

2.1.2 **Cameras**. To protect access to Martin Defense Group premises outside of normal business hours, the FSO and/or Office Manager shall install cameras to record images of personnel who approach Martin Defense Group's doors (& data kept for three years) as well as an alarm system that Users will arm when they close Martin Defense Group's office.

2.1.3 **Visitor log**. Users who invite non-Martin Defense Group personnel onto Martin Defense Group premises shall have these visitors fill out a visitor log with their name, company, contact information, national citizenship, and name of User who authorized access and continuously escort these visitors until they leave Martin Defense Group's premises.

(1) Users shall give visitors badges that expire and visibly distinguishes them from Users.

(2) Visitors shall return the visitor badge to the User before leaving Martin Defense Group premises.

2.2 **Access to Media**

2.2.1 **Physical Access**

(1) Users who handle documents containing CUI should store them in locked drawers at the end of the day as well as take measures to cover such information when stepping away from their desk.

(2) For procedures related to printing documents containing CUI, see the AC-104 Printing in a Network Environment procedures.

(3) Designated IT Personnel, Officer Manager, and/or FSO shall protect access to the fileservers by keeping the door to the room containing them locked at all times.

2.2.2 **Logical Access**

(1) Designated IT Personnel may only provide access to information on the Restricted network server and the SharePoint platform to Users who are authorized after following the AC-100 Account Management procedures.

(2) Designated IT Personnel must encrypt all CUI stored on digital media under FIPS 140-2 level encryption.

2.3 **Changes to Systems**

2.3.1 Users are not allowed to make any physical additions, modifications, and removals of Martin Defense Group-issued hardware or software applications. Users who need such changes should e-mail Martin Defense Group IT <IT@mdefensegroup.com> to request such changes. Designated IT Personnel shall make such changes.

2.4 **Offsite Access**

2.4.1 To prevent CUI from being transferred to non-Martin Defense Group equipment, Users may not install printer drivers to non-Martin Defense Group printers and other software drivers that allow Users to transfer information from their laptops to non-Martin Defense Group wireless devices.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 FSO and/or Officer Manager. Ensure that:

(1) Secure areas are protected by appropriate entry and controls for authorized personnel.

(2) Procedures control and validate a staff member's access to facilities with the use of security personnel, identification badges, or electronic key cards.

(3) Procedures exist that establish visitor controls including visitor sign-in logs and the wearing of visitor badges for both entry and exit of the Martin Defense Group LLC.

(4) Policies specify management's review of the list of individuals with physical access to facilities containing sensitive information (whether in paper or electronic forms)
(5) A complete inventory of critical assets is maintained with Martin Defense Group ownership defined and documented.
(6) Card access records and visitor logs for facilities are kept for at least three years and reviewed at least every 90 days.

3.1.2 Designated IT Personnel. Responsible for:

(1) Implementing physical and/or logical controls to restrict access to publicly accessible data jacks.

(2) Restricting physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines for only Users.

(3) Controlling physical and logical access to diagnostic and configuration ports.

3.2 **Definitions**. See Appendix C Glossary.

SOP #:	**MDG-PHYS-101**
Title:	**Physical Access Devices**

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to specify the processes used to control and manage physical access devices issued to individuals with authorized access to Martin Defense Group facilities.

2.0 Procedure

2.1 **Acquiring Access Cards/Keys**. Users who wish to access Martin Defense Group's premises must contact the FSO or Officer Manager to obtain access cards and/or keys to unlock the locks on Martin Defense Group's doors.

2.1.1 Employee access cards and/or keys must not be shared or loaned to others

2.2 **Reporting Lost or Stolen Cards/Keys**. Lost or stolen cards/or keys must be reported immediately to the FSO or Office Manager.

3.0 Reference

3.1 **Roles and Responsibilities**

3.1.1 FSO or Officer Manager. Stores all spare access codes and/or keys to Martin Defense Group's doors in a locked container, maintains a log of Users who have an access card and/or key, inventories physical keys at least annually, and changes combinations and keys when access cards or keys are lost, combinations are compromised, or individuals are transferred or terminated. Reviews access records and visitor logs for the facility annually and investigate any unusual events or incidents related to physical facility access.

3.2 **Definitions**. See Appendix C Glossary.

Systems Maintenance Policy

32 Overview

Properly maintaining organization information systems is a critical component of information security. Maintaining systems and data reduces the potential for harming Martin Defense Group through data theft, malware installation, and system damage. To that end, maintenance of organization systems, including but not limited to laptop computers, desktop computers, servers, mobile devices, and network devices, is to be managed according to rules set forth in this document.

Effective security is a team effort involving the participation and support of every Martin Defense Group User and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to support the security precepts in these guidelines and to conduct their activities accordingly.

33 Purpose

The purpose of this policy is to outline the required and acceptable methods for maintaining information systems at Martin Defense Group. These rules are in place to protect a User and Martin Defense Group. Circumventing or avoiding systems maintenance procedures exposes Martin Defense Group to risks including virus attacks, compromise of network systems and services, and legal liability.

34 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Martin Defense Group business or interact with internal networks and business systems, whether owned or leased by Martin Defense Group, a User, or a third party. All Martin Defense Group Users and its subsidiaries are required to access Martin Defense Group computers and systems in accordance with Martin Defense Group policies and standards, and local laws and regulations. Definitions to terms are provided in Appendix C Glossary.

35 Policy

Martin Defense Group:

a. Performs maintenance on organizational systems. (3.7.1)[13]

    1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (MA-2a)
    2. Uses a maintenance log to capture all system component maintenance that includes: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance

[13] Numbers in parentheses indicate a cross-reference to NIST SP 800-171 (beginning with a number, e.g., “3.1.1”) and/or NIST SP 800-53 (beginning with a letter, e.g., “AC-2”).

performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). (MA-2)

b. Provides effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. (3.7.2)

    1. Approves and monitors all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location. (MA-2b)
    2. Requires that system/network administrator designate or explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. (MA-2c)
    3. Approves, controls, and monitors information system maintenance tools. (MA-3)
    4. Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. (MA-3(1))
    5. Checks media containing diagnostic and test programs for malicious code before the media are used in the information system. (MA-3(2))

c. Ensures equipment removed for off-site maintenance is sanitized of any CUI using a NIST-approved sanitization tool (see Media Protection and Backup Policy) or removing the media containing CUI. (3.7.3, MA-2d)

d. Checks media containing diagnostic and test programs for malicious code before the media are used in organizational information systems. (3.7.4, MA-3(2))

e. Requires multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminates such connections when nonlocal maintenance is completed. (3.7.5)

    1. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; (MA-4c)
    2. Maintains records for nonlocal maintenance and diagnostic activities (MA-4d)
    3. Terminates session and network connections when nonlocal maintenance is completed via an automatic SSL VPN tunnel termination set to 15 minutes of inactivity. (MA-4e)

f. Supervises the maintenance activities of maintenance personnel without required access authorization. (3.7.6)

    1. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations (MA-5b)
    2. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. (MA-5c)

g. The current ticketing system will be utilized to document all system changes. This will provide not only an audit of individual requests, and maintenance changes made by the IT department.

SOP #:	MDG-AT-100
Title:	Awareness & Training Plan

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

2.0 Procedure

2.1 **User training**

2.1.1 Designated IT Personnel shall provide training to Users on the following topics on an annual basis:

(1) Security awareness
  (a) This training shall include discussion that personal portable storage devices and other devices with no identifiable owner are prohibited from being connected to Martin Defense Group's information systems.
(2) Security-related duty and responsibility
(3) Recognizing and reporting potential indicators of insider threat

2.1.2 Designated IT Personnel shall provide training to Users annually on interacting with the media regarding cyber incidents, including the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.

(1) Designated IT Personnel shall establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.

(2) All Users shall be informed of general procedures for handling media inquiries developed in paragraph (1) above.

2.2 **Incident Response Team training**

2.2.1 Members of the IRT shall receive training within 30 days of assuming the role and be trained annually on interacting with the media regarding cyber incidents, including the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.

2.2.2 Within 30 days of assuming the role, the FSO and/or Officer Manager who is responsible for being the law enforcement point of contact shall receive training on the reporting procedures for all relevant law enforcement agencies and on recommending which agency, if any, should be contacted.

3.0 Reference

3.1 **Definitions**. See Appendix C Glossary.

Policy Compliance

1. Compliance Measurement

Martin Defense Group will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the IT Steering Committee in advance.

3. Non-Compliance

A User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Version	Revision Date	Revised By	Revision Notes
1.0			Initial Version

Appendix C. Glossary

Adverse Event. An event with a negative consequence. Adverse events include, but are not limited to, system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Authentication. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticator. The means used to confirm the identity of a user, processor, or device (e.g., user password or token). Throughout this SOP, we will use "password" interchangeably with "authenticator."

Collaborative computing device. Collaborative computing devices include, for example, networked white boards, cameras, and microphones.

Computer Security Incidents (Incidents). Violations or imminent threat of violation[14] of computer security policies, acceptable use policies, or standard security practices. Examples of incidents[15] are:

1. An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
2. Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
3. An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
4. A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Controlled Unclassified Information (CUI) means unclassified controlled information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. (DFARS 252.204-7012(a))

Cyber incident. "Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

[14] An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet.

[15] For the remainder of this document, the terms "incident," "computer security incident," and "cyber incident" are interchangeable.

Cybersecurity events are any observable occurrence in a system or network. Events include, but are not limited to, a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Cybersecurity adverse events are events with a negative consequence. Adverse events include, but are not limited to, system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Direct Access. Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a wired connection (Ethernet cable or similar) from the host to the network.

Event. Any observable occurrence in a system or network. Events include but are not limited to a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Incident Response Team. This is the set of Martin Defense Group staff that have been designated to respond to cyber incidents.

Information System [44 U.S.C., Sec. 3502]. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *Note*: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Media. Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Mobile Device. A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, E-readers, and notebook computers.

Multifactor Authentication. This requires two or more different factors to achieve authentication. The factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

Physical access devices. Physical access devices include, for example, keys, locks, combinations, access cards, proximity access cards, and keyfobs, and card readers.

Portable Storage Device. An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video,

audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Privileged Account. An information system account with authorizations of a privileged user.

Privileged User. A user who is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Publicly Accessible. An information system that is accessible to the general public without restriction, typically without identification or authentication.

Remote Access. Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

System-level information. System-level information includes, for example, system-state information, operating system and application software, and licenses.

User-level information. User-level information includes any information that is not system-level information.

User. An employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization, who has been granted access to and employs the information system for business purposes.

Wireless Access. Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through radio transceivers complying with standards such as IEEE 802.11x or Bluetooth. Typically associated with mobile devices.

Exhibit 4

MARTIN DEFENSE GROUP
841 Bishop St., Suite 1110, Honolulu, HI 96813

MDG Employee Mobile Device Policy

This policy applies to any Company-supplied device that makes/receives phone calls, leaves messages, sends text messages, surfs the internet, or allows for the use of email.

Company Owned and Supplied Devices

- The Company will provide all full-time staff with an IT-approved standard-issue mobile device as soon as practicable after the start of employment, though the Company management reserves the right to make exceptions for any reason.
- The Company owns any and all phone numbers for accounts that are paid for by the Company.
- Employees are eligible to upgrade beyond the standard-issue device or provide their own non-standard device at their own expense, provided the device conforms to the Company's IT/Security policy requirements.
- The Company provides a mobile device as both a necessity for the regular and complete execution of the employee's professional responsibilities and a benefit for the employee.
- The employee will be responsible for Company-provided equipment and shall make reasonable efforts to:
    - Keep the equipment free of damage beyond normal wear and tear from regular use;
    - Protect their own personal data, as the Company will not responsible for personal data loss; and
    - Protect the equipment from loss, theft and unauthorized access by non-Company personnel.
- At any time upon request by Company management, the employee shall produce the mobile device for return or inspection.
- Failure to comply with these policies may be cause for disciplinary action, up to and including termination of employment.
- Upon termination or departure from the Company, the employee's mobile device may be purchased at fair value (as determined by the Company), and if so desired by the employee, the phone line may be released to the employee.

Objective

This policy outlines the use of mobile devices, both personal and Company-provided, for work and work-related purposes as well as recommended practices for the safe use of mobile devices by employees. This policy applies to all employees.

Policy Elements

Despite their benefits, mobile devices may cause problems in the workplace. Employees who use their mobile devices inappropriately may:

- Get distracted from their work.
- Disturb colleagues.
- Expose the Company to security issues from inappropriate usage.
- Cause accidents when using their mobile devices while their attention should be focused elsewhere during potentially dangerous activities such as driving or working near heavy machinery.

The company expects employees to use their mobile devices prudently during working hours.

MARTIN DEFENSE GROUP
841 Bishop St., Suite 1110, Honolulu, HI 96813

We advise our employees to:

- To use prudent judgement and common courtesy when using mobile devices.
- Use company-issued mobile devices primarily for business purposes and preserve them in the condition received, allowing for minor wear and tear.
- Turn off or silence their mobile devices when asked or as appropriate to the situation.
- To place mobile devices on silent or vibrate mode during meetings, conferences, and in any circumstance where incoming calls or notifications may be disruptive.

We do not condone the:

- Use of cameras or other video/audio recording-capable devices on Company premises without the prior permission of senior management.
- Use of mobile devices for any reason while driving or working near heavy machinery.
- Recording proprietary information for purposes not directly related to work.
- Use of mobile devices in areas where cell use is explicitly prohibited (e.g. laboratories or specific government facilities prohibiting the use of cell phones.)
- Download or upload of inappropriate, illegal, or obscene material.
- Use of mobile devices in any way which interferes with the fulfillment of an employee's work priorities and assignments or places the employee or others at risk of physical harm.

We encourage the use of mobile devices:

- For appropriate business communication.
- To increase work efficiency with productivity applications.
- To maintain necessary work continuity and progress outside of regular business hours.
- To attend to urgent personal matters to allow the employee to maintain focus on work.

Disciplinary Consequences

The Company retains the right to monitor employees for excessive or inappropriate use of their mobile devices. If an employee's usage causes a prolonged decline in productivity or interferes with our operations, the Company may ban that employee from using mobile devices during business hours and/or repossess a Company-provided mobile device.

Employees may face severe disciplinary action up to and including termination, in cases when they:

- Violate the Company's security policies.
- Breach the Company's confidentiality policies.
- Cause an incident harmful to the Company's interests or reputation.

The undersigned employee acknowledges that he or she has read the MDG Employee Mobile Device Policy and agrees to comply with all terms of the policy.

_____ _____

EMPLOYEE DATE

Exhibit 5

verizon

PO BOX 489
NEWARK, NJ 07101–0489

Manage Your Account	Account Number	Date Due
www.vzw.com/mybusinessaccount	[redacted]	01/12/20
Change your address at http://sso.verizonenterprise.com	Invoice Number	9844643362

KEYLINE

NAVATEK LLC
841 BISHOP ST STE 1110 DA
SUITE 1110
HONOLULU, HI 96813

Quick Bill Summary

Nov 22 – Dec 20

Previous Balance *(see back for details)*	$.00
No Payment Received	$.00
Balance Forward	**$.00**
Account Charges and Credits	$534.90
Monthly Charges	$9,844.92
Usage and Purchase Charges	
Voice	$.49
Messaging	$.00
Data	$.00
Equipment Charges	$1,373.16
Surcharges and Other Charges & Credits	$1,184.37
Taxes, Governmental Surcharges & Fees	$153.12
Total Current Charges	**$13,090.96**

Total Charges Due by January 12, 2020 **$13,090.96**

Verizon Wireless News

New Activation Message

Welcome to Verizon Wireless! Your first bill may include charges for a partial month of service, plus your first full month's access charge billed one month in advance.

Pay from phone	Pay on the Web	Questions:
#PMT (#768)	At vzw.com/mybusinessaccount	1.800.922.0204 or *611 from your phone

verizon

NAVATEK LLC
841 BISHOP ST STE 1110 DA
SUITE 1110
HONOLULU, HI 96813

Bill Date December 20, 2019
Account Number [redacted]
Invoice Number 9844643362

Total Amount Due by January 12, 2020

Make check payable to Verizon Wireless.
Please return this remit slip with payment.

$13,090.96

$☐☐,☐☐☐.☐☐

PO BOX 660108
DALLAS, TX 75266–0108

[redacted]

NOTICE: Bank account and routing numbers will be retained to enable future payments by phone or online. To opt out, call 1–866–544–0401.

Exhibit 5

verizon

Invoice Number	Account Number	Date Due	Page
9844643362	[redacted]	01/12/20	122 of 162

Summary for Martin Kao: [redacted]-0371

Your Plan

Plan from 11/25 – 12/20
Business Unlimited Smartphone
$45.00 monthly charge
Unlimited monthly minutes

UNL Text Messaging
Unlimited M2M Text
Unlimited Text Message

Plan from 11/25 – 12/20
Email & Web Unlimited
Unlimited monthly gigabyte

UNL Picture/Video MSG
Unlimited monthly Picture & Video

Have more questions about your charges? Get details for usage charges at www.vzw.com/mybusinessaccount.

Monthly Charges

New Plan

Business Unlimited Smartphone	11/25 – 12/20	39.00
$45.00 per month / 26 days on new plan		

Month in Advance

Business Unlimited Smartphone	12/21 – 01/20	45.00
These are the normal monthly charges billed in advance.		
		$84.00

Equipment Charges

Equipment Purchase	11/26 Vbg – Direct Sales –	001747473	52.36
Equipment Purchase	11/26 Vbg – Direct Sales –	001747473	52.36
Equipment Purchase	11/26 Vbg – Direct Sales –	001747473	52.36
Device Payment Agreement 1313506811 – Payment 1 of 24			48.06
Balance (after this month's current payment) 1101.93			
HI General Excise Surcharge		(one–time charge)	54.19
			$259.33

Usage and Purchase Charges

Voice		Allowance	Used	Billable	Cost
Calling Plan (11/25 – 12/20)	*minutes*	unlimited	212	--	--
Total Voice					$.00

Messaging		Allowance	Used	Billable	Cost
Text (11/25 – 12/20)	*messages*	unlimited	39	--	--
Unlimited M2M Text (11/25 – 12/20)	*messages*	unlimited	13	--	--
Picture & Video – Sent (11/25 – 12/20)	*messages*	unlimited	53	--	--
Picture & Video – Rcv'd (11/25 – 12/20)	*messages*	unlimited	11	--	--
Total Messaging					$.00

Data		Allowance	Used	Billable	Cost
Gigabyte Usage(11/25 – 12/20)	*gigabytes*	unlimited	14.762	--	--
Total Data					$.00

Total Usage and Purchase Charges **$.00**

Surcharges

Fed Universal Service Charge	1.15
Regulatory Charge	.30
Administrative Charge	3.56
HI Telecom Relay Surchg	.04
HI Public Srvc CO Surcharge	1.40

verizon

Invoice Number	Account Number	Date Due	Page
9844643362	[redacted]	01/12/20	123 of 162

Monthly Charges, continued

Surcharges

HI State PUC Fee	.10
HI Gen Excise Surchg–Telecom	3.02
	$9.57

Taxes, Governmental Surcharges and Fees

HI State 911 Surcharge	1.32
	$1.32

Total Current Charges for 808–371–0371 **$354.22**

Detail for Martin Kao: 808–371–0371

Voice

Date	Time	Number	Rate	Usage Type	Origination	Destination	Min.	Airtime Chrgs	LD/Other Chrgs	Total
12/05	12:31A	[redacted]4285	Off–Peak	PlanAllow	Stillwater OK	Honolulu HI	3	—	—	—
12/05	11:08P	[redacted]4285	Off–Peak	PlanAllow	Oklahoma C OK	Honolulu HI	1	—	—	—
12/05	11:08P	[redacted]4285	Off–Peak	PlanAllow	Oklahoma C OK	Incoming CL	21	—	—	—
12/08	5:22P	[redacted]0056	Off–Peak	PlanAllow	Honolulu HI	Honolulu HI	4	—	—	—
12/09	8:43A	[redacted]8106	Peak	PlanAllow	Honolulu HI	Incoming CL	2	—	—	—
12/09	3:37P	[redacted]6394	Peak	PlanAllow	Honolulu HI	Incoming CL	1	—	—	—
12/10	8:11A	[redacted]4285	Peak	PlanAllow	Honolulu HI	Incoming CL	2	—	—	—
12/10	9:19A	[redacted]4285	Peak	PlanAllow	Honolulu HI	Incoming CL	4	—	—	—
12/10	9:30A	[redacted]5932	Peak	PlanAllow	Honolulu HI	Incoming CL	30	—	—	—
12/10	10:11A	[redacted]4285	Peak	PlanAllow	Honolulu HI	Honolulu HI	3	—	—	—
12/10	12:33P	[redacted]8905	Peak	PlanAllow	Honolulu HI	Honolulu HI	1	—	—	—
12/10	5:13P	[redacted]4285	Peak	PlanAllow	Honolulu HI	Incoming CL	2	—	—	—
12/11	10:31A	[redacted]3852	Peak	PlanAllow	Honolulu HI	Wshngtnzn1 DC	24	—	—	—
12/11	11:31A	[redacted]7001	Peak	PlanAllow	Honolulu HI	Honolulu HI	19	—	—	—
12/11	4:38P	[redacted]4285	Peak	PlanAllow	Honolulu HI	Incoming CL	2	—	—	—
12/11	4:45P	[redacted]4285	Peak	PlanAllow	Honolulu HI	Honolulu HI	1	—	—	—
12/11	4:47P	[redacted]4285	Peak	PlanAllow	Honolulu HI	Incoming CL	1	—	—	—
12/12	10:36A	[redacted]4285	Peak	PlanAllow	Honolulu HI	Honolulu HI	3	—	—	—
12/12	3:01P	[redacted]0559	Peak	PlanAllow	Honolulu HI	Incoming CL	1	—	—	—
12/13	8:56A	[redacted]9984	Peak	PlanAllow	Honolulu HI	Wshngtnzn1 DC	34	—	—	—
12/13	3:10P	[redacted]0559	Peak	PlanAllow	Honolulu HI	Incoming CL	1	—	—	—
12/16	9:14P	[redacted]3433	Off–Peak	PlanAllow,M2M	Washington DC	Honolulu HI	12	—	—	—
12/16	10:40P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	Honolulu HI	25	—	—	—
12/16	11:58P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	Incoming CL	2	—	—	—
12/17	11:23P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	VM Deposit CL	1	—	—	—
12/17	11:34P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	Incoming CL	6	—	—	—
12/18	10:22P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	VM Deposit CL	1	—	—	—
12/19	10:46P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	VM Deposit CL	1	—	—	—
12/19	11:36P	[redacted]4285	Off–Peak	PlanAllow	Washington DC	Incoming CL	4	—	—	—

Exhibit 6

KOBAYASHI SUGITA & GODA, LLP
Attorneys at Law

Bert T. Kobayashi, Jr.*
Alan M. Goda*

John R. Aube*
Charles W. Gall*
Neal T. Gota
Clifford K. Higa*
Charles D. Hunter
Robert K. Ichikawa*
Christopher T. Kobayashi*
Jonathan A. Kobayashi
Jan M. L. Y. Kutsunai*
David M. Louie*
Nicholas R. Monlux
Jonathan S. Moore
Aaron R. Mun
Bruce A. Nakamura*

Kenneth M. Nakasone*
Gregory M. Sato*
Jesse W. Schiel*
Craig K. Shikuma*
Lex R. Smith*
Joseph A. Stewart*
Brian D. Tongg
David B. Tongg*
Caycie K. G. Wong

*A Law Corporation

Of Counsel:
Kenneth Y. Sugita*
Wendell H. Fuji*
Burt T. Lau*
John F. Lezak*
Larry L. Myers*
David Y. Suzuki*
Maria Y. Wang

Kaylee K. Correa
Sianha M. Gualano
Austin H. Jim On
Stephen G. K. Kaneshiro
Travis Y. Kuwahara
Ryan D. Louie
Chelsea C. Maja

December 21, 2022

Via E-mail

Craig Nolan, Assistant United States Attorney
craig.nolan@usdoj.gov
United States Attorney's Office for the District of Hawaii
Room 6100, PJKK Federal Building
Honolulu, Hawaii 96850

Re: *United States v. Martin Kao*
Case No. 1:21-cr-00061 (LEK) (the "**Criminal Case**")

Dear Mr. Nolan:

As you know, we represent PacMar Technologies LLC f/k/a Martin Defense Group, LLC f/k/a Navatek LLC ("**PacMar**" or the "**Company**") and Steven Loui. We write to request the Department of Justice's ("**DOJ**") assistance related to the recovery of certain Company property seized by the DOJ from Defendant Martin Kao ("**Defendant Kao**").

In 2020, around the time the DOJ arrested Defendant Kao, it seized various property, including certain Company property[1], potentially relevant to Mr. Kao's crimes in the Criminal Case. Among the items seized was an Apple iPhone 11 Pro (IMEI 353247100759018) associated with the phone number ending in 0371 ("**Mr. Kao's Company Cellphone**"). Mr. Kao's Company Cellphone was registered to a Company business account assigned to Defendant Kao.

Pursuant to the Company's employment policies in effect at the time (which remain in effect), Company cellphones and computers used by its employees, including Mr. Kao's Company Cellphone and the content and records therein, are Company property. For the

[1] The DOJ returned most of the Company assets seized, including the Company's servers, shortly after they were downloaded.

avoidance of doubt, this includes all forms of data related to the communications and applications stored thereon, which includes but is not limited to the call logs, voice message data, text messages, e-mails, and other forms of messaging; still and live photographs and video; audio files; storing dates, appointments, and other information on personal calendars, among other data (collectively, the "**Cellphone Data**").

Unlike servers and other property temporarily seized by the DOJ that have since been returned to the Company, the Company has no record of the DOJ returning either Mr. Kao's Company Cellphone or the Cellphone Data to the Company.

The Company therefore requests that the DOJ return Mr. Kao's Company Cellphone and/or the Cellphone Data to the Company as soon as possible. To the extent the DOJ desires to maintain possession of Mr. Kao's Company Cellphone as physical evidence in its pending Criminal Case, the DOJ's return of the extracted Cellphone Data through a searchable reader (i.e., CelleBrite) will suffice in lieu of a return of the physical Cellphone.

Your immediate attention and assistance concerning this request is appreciated. Please do not hesitate to contact me should you have any questions.

Very truly yours,

DAVID M. LOUIE
JESSE W. SCHIEL
for
KOBAYASHI, SUGITA & GODA, LLP

Exhibit 7

On Thursday, December 29, 2022 at 08:02:41 AM HST, Nolan, Craig (USAHI) <craig.nolan@usdoj.gov> wrote:

Victor,

In the attached letter counsel to PacMar (copied), f/k/a Martin Defense Group, f/k/a Navatek, requests that the government return to PacMar the iPhone seized from Mr. Kao in connection with his September 2020 arrest or, alternatively, the data contained in the iPhone. PacMar asserts that the iPhone and data are PacMar's property. Because the prosecution against Mr. Kao remains pending and the iPhone constitutes and contains evidence, the government has informed PacMar's counsel that the government will not return the iPhone at this time, but is willing to provide PacMar with the data forensically extracted from the phone. The government explained further that it would provide an opportunity for Mr. Kao to object to a production of the data to PacMar on the basis that the iPhone or the data contained within the iPhone is Mr. Kao's personal property or that Mr. Kao possesses a privacy interest in the data under the applicable policies of or his employment agreement with PacMar.

By 5:00 p.m., Friday, January 6, 2023, please notify me whether Mr. Kao objects to the requested production of iPhone data to PacMar. If Mr. Kao objects, I will confer with counsel for PacMar and you about the best manner in which to get the dispute before the Court.

Sincerely,

Craig S. Nolan

Assistant United States Attorney

District of Hawaii

300 Ala Moana Blvd., Rm. 6-100

Honolulu HI 96850

(808) 754-9681 (mobile)

(808) 440-9225 (direct)

(808) 541-2850 (main)

(808) 541-2958 (fax)

Craig.Nolan@usdoj.gov

Exhibit 7

Exhibit 8

From: vbakke@bakkelawfirm.com <vbakke@bakkelawfirm.com>
Sent: Thursday, January 5, 2023 5:07 PM
To: Nolan, Craig (USAHI) <CNolan@usa.doj.gov>
Cc: Warren Fabro - Bakke Law Office (wfabro@bakkelawfirm.com) <wfabro@bakkelawfirm.com>
Subject: [EXTERNAL] Re: US v. Kao - Request by Company for Return of

Craig. Sorry, I forgot to ask you about this when we spoke a few minutes ago. I have discussed this matter with Mr. Kao and we respectfully object to the Government turning over the physical phone and/or any of the associated data, images, text, emails, meta data, etc. to PAC-MAR or any other person or entity.

Sincerely, Victor J. Bakke, Esq.

Law Office of Victor Bakke
Topa Financial Center
700 Bishop Street, Ste. 2100
Honolulu, HI 96813
Office phone: 808-369-8170
Cell phone: 808-349-9757
Fax: 808-369-8179
Web site: ArrestedHawaii.com

Exhibit 8

Exhibit 9

From: Nolan, Craig (USAHI) <Craig.Nolan@usdoj.gov>
Sent: Friday, January 6, 2023 5:33 AM
To: vbakke@bakkelawfirm.com; Jesse W. Schiel <jschiel@ksglaw.com>
Cc: Warren Fabro - Bakke Law Office (wfabro@bakkelawfirm.com) <wfabro@bakkelawfirm.com>
Subject: RE: [EXTERNAL] Re: US v. Kao - Request by Company for Return of

Victor and Jesse,

Please let me know whether a phone call or meeting of the three of us would assist in resolving the dispute (memorialized below) about production to PacMar of the data extracted from the iPhone seized pursuant to warrant from Martin Kao in September 2020. If not, I suggest we get the issue before Judge Kobayashi by PacMar filing a motion for return of property, i.e., the extracted data, pursuant to Fed. R. Crim. P. 41(g). In response to such a motion, the government will take no position (other than opposing the request to the extent that it seeks return of the actual iPhone).

Sincerely,

Craig S. Nolan
Assistant United States Attorney
District of Hawaii
300 Ala Moana Blvd., Rm. 6-100
Honolulu HI 96850
(808) 754-9681 (mobile)
(808) 440-9225 (direct)
(808) 541-2850 (main)
(808) 541-2958 (fax)
Craig.Nolan@usdoj.gov

Exhibit 9

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. MARTIN KAO, Defendant.	CR. NO. 21-00061 LEK CERTIFICATE OF SERVICE

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on the date noted below, a copy of the foregoing document was duly served on the following parties via CM/ECF:

JENNIFER BILINKAS — Jennifer.Bilinkas@usdoj.gov
CRAIG S. NOLAN — craig.nolan@usdoj.gov
U.S. Department of Justice
District of Hawaii
300 Ala Moana Blvd., #6-100
Honolulu, Hawaii 96850

Attorney for Plaintiff
UNITED STATES OF AMERICA

VICTOR J. BAKKE — vbakke@bakkelawfirm.com
Law Office of Victor Bakke
Topa Financial Center
700 Bishop Street, Suite 2100
Honolulu, Hawaii 96813

Attorney for Defendant
MARTIN KAO

DATED: Honolulu, Hawaii, January 24, 2023.

/s/ Jesse W. Schiel
DAVID M. LOUIE
JESSE W. SCHIEL

Attorneys for Movant
PACMAR TECHNOLOGIES LLC
f/k/a MARTIN DEFENSE GROUP,
LLC f/k/a NAVATEK LLC