CIVIL SERVICE COMMISSION
Kumision I Setbision Sibit
GOVERNMENT OF GUAM
I Gobietnon Guahan
Bell Tower, Suite 201
710 West Marine Corps Drive
Hagatna, Guam 96910
Tel: (671) 647-1855/1857 • Fax: (671) 647-1867
Website: csc.guam.gov

LOURDES A. LEON GUERRERO
Governor
JOSHUA F. TENORIO
Lieutenant Governor

DANIEL D. LEON GUERRERO
Executive Director

CIVIL SERVICE CO

22-281

04 28 2022
10:35AM
RECEIVED

Employee Address and Contact Information / Disclosure Form:

This form requests information that is relevant and necessary to reach a decision in your Appeal. The Civil Service Commission collects this information in order to process Appeals or Complaints under its statutory and regulatory authority. An Appeal or Complaint is a voluntary action, you are not required to provide any personal information in connection with it. However, failure to supply the Civil Service Commission with all the information essential to reach a decision in your case could result in the rejection of your Appeal or Complaint.

Please be advised that your Appeal or Complaint is available to the public under the provisions of the Sunshine Reform Act of 1999. Information contained in your Appeal or Complaint file may be released as required by the Sunshine Reform Act of 1999. Additionally, information about your Appeal or Complaint will also be used in a depersonalized form in a database for program statistics.

Please print legibly below:

Employee Name:	LEO RUSTUM J. ESPIA
Position Title:	PLANNER IV
Agency/Department:	GUAM HOMELAND SECURITY/OFFICE OF CIVIL DEFENSE
Home Phone:	[redacted]
Work Phone:	(671) 475-9600
Cell Phone:	[redacted]
Home Address:	[redacted]
Mailing Address:	[redacted]
E-mail address:	[redacted]

DISCLOSURE OF INFORMATION: **Upon filing of any Appeal or Complaint, all documents submitted to the Civil Service Commission become public records/writing. The documents may be disclosed, inspected, or copied pursuant to the Sunshine Reform Act (5GCA, Chapter 10) or other applicable law(s). Personal information will not be made available to the public (i.e., SSN#, home address, etc.).**

I hereby agree and acknowledge that upon any changes of the above information, I will notify the Commission. Non-notification may result in my case being dismissed. Furthermore, I have read and understand the Disclosure of Information Statement above.

SIGNATURE & DATE OF EMPLOYEE	SIGNATURE & DATE OF REPRESENTATIVE
04/27/2022	Robert Kess 487-4007 4/27/22

COPY

CIVIL SERVICE COMMISSION
Kumision I Setbision Sibit
GOVERNMENT OF GUAM
I Gobietnon Guahan
Bell Tower, Suite 201
710 West Marine Corps Drive
Hagatna, Guam 96910
Tel: (671) 647-1855/1857 • Fax: (671) 647-1867
Website: csc.guam.gov

LOURDES A. LEON GUERRERO
Governor
JOSHUA F. TENORIO
Lieutenant Governor

DANIEL D. LEON GUERRERO
Executive Director

DATE: APRIL 27, 2022

TO: Executive Director, Civil Service Commission

FROM: LEO RUSTUM J. ESPIA

SUBJECT: ☑ Letter of Appeal ☐ Letter of Complaint
(Must check only one (1) item. For multiple Appeals or Complaints please fill out additional forms.)

APPEAL: (Please check only one (1) box)
☑ **Adverse Action** ☐ **Grievance** ☐ **Equal Employment Opportunity**
☐ **Lay-Off "Bad Faith"** ☐ **Furlough "Bad Faith"** ☐ **Priority Placement "Bad Faith"**

COMPLAINT: (Please check only one (1) box)
☐ **Post Audit** ☐ **Notice of Personnel Action** ☐ **Lay-Off** ☐ **Furlough** ☐ **Priority Placement**
☐ **Public Protection Act, "AKA: Whistle Blower"** ☐ **Ethics in Procurement** ☐ **Political Activity, "AKA: Mini-Hatch"**

I, LEO RUSTUM J. ESPIA
(Print Full Name)

A ☑ Classified employee ☐ Unclassified Employee of GUAM HOMELAND SECURITY/ OFFICE OF CIVIL DEFENSE in the position
(Agency or Department)

PLANNER IV, alleges that the action is inappropriate for the following reasons:
(Your official job title)

ADVERSE ACTION WAS TAKEN WITHOUT CAUSE. THERE IS NO MALFEASANCE OR MISCONDUCT. ADVERSE ACTION PROCEDURALLY DEFECTIVE AND TAKEN IN VIOLATION OF GUAM LAWS AND RULES.

04/27/2022
Signature & Date

GOVERNMENT OF GUAM
AGANA, GUAM 96910

NOTICE OF FINAL ADVERSE ACTION

NAME OF EMPLOYEE:
LEO R. ESPIA

SOCIAL SECURITY NUMBER:
XXX-XX-1253

POSITION TITLE:
PLANNER IV

DEPARTMENT/DIVISION:
GUAM HOMELAND SECURITY/OFFICE OF CIVIL DEFENSE

DATE OF THIS ACTION: APRIL 26, 2022

LAST KNOWN RESIDENCE/MAILING ADDRESS: [redacted]

PHYSICAL ADDRESS: [redacted]

MAILING ADDRESS/HOME DELIVERY:

TYPE OF ACTION:

/ / Notice of Proposed Adverse Action (note: Employee must answer orally or in writing within ten (10) calendar days after receipt of this notice.

/X/ Notice of Final Adverse Action

A. SUSPENSION

Effective:

Number of Working Days:

You may appeal this action in accordance with the procedure outlined on page four (4).

B. DEMOTION

FROM:

TO:

You may appeal this action in accordance with the procedure outline on page four (4).

C. DISMISSAL*****

Effective: Immediately COB April 26, 2022**

You may appeal this action in accordance with the procedure outlined on page four (4).

NOTE: A Request for Personnel Action (GG-1) is required to effectuate an Adverse Action.

THIS ACTION IS TAKEN IN ACCORDANCE WITH CHAPTER 11.303, PERSONNEL RULES AND REGULATIONS, EXECUTIVE ORDER 96-24 "AUTHORIZED CAUSES FOR ADVERSE ACTION" AS SHOWN AND MARKED BELOW:

/ / A. Fraud in securing appointment

/X / B. Refusal or failure to perform prescribed duties and responsibilities

/X / C. Insubordination (refusal to attend meeting with Director February 18, 2022 and answer emails and orders from Director).

/ / D. Intoxication while on duty or the unauthorized possession, use or sale of alcohol on duty on while on government premises.

/ / E. Unlawful *use, possession*, or sale of illicit drugs

/X/ F. Unauthorized absences (February 18, 2022)

/ / G. Conviction of a crime.

/X / H. Discourteous treatment to the public or other employees.

/ / I. Political activity prohibited by law.

/X/ J. Misuse or theft of government property misuse of official and confidential information, government email (sensitive but non classified information), misuse of his government office and position, and government equipment).

/ / K. Refusal to take and subscribe to any oath or affirmation which is required by law in connection with employment.

/ / L. Acts prohibited by Section 9102, 4 GCA relating to strikes against the government.

/ / M. Acts of prohibited discrimination to include sexual harassment.

/ / N. Failure to comply with the Drug-Free Workplace Program (positive drug test).

/X/ O. Other misconduct not specifically listed [improperly disclosing confidential or government information without authorization, criminal conduct (official misconduct, tampering with records, unethical conduct; notoriously disgraceful conduct (on duty or off duty) adversely affecting employer/employee relationship, dishonest conduct, making false and misleading statements to investigators, attempt to conceal misconduct, and discourteous and disrespectful conduct. Violation of Chapter 3 DOA PR&R Code of Conduct.

*See supporting facts and circumstances below to support each of the charges indicated. These were also set forth in the proposed adverse action.

/ / Chapter 11.306, PR&R, EO96-24 NOTICE OF PROPOSED ADVERSE ACTION

An employee against whom adverse action is sought is entitled to immediate written notice stating any and all reasons, specifically and in detail, for the proposed action. The written notice must make it clear that it concerns only proposed action and not a matter already decided. A copy of such action shall be filed by the department/agency head with the Department of Administration and the Civil Service Commission (CSC).

/ / Chapter 11.307, PR&R, EO96-24 EMPLOYEE'S ANSWER

An employee is entitled to seek reconsideration of the proposed adverse action by answering any charges within 10 days after receipt of the notice; the answer may be made orally, in writing, or both. The department/agency head shall be available to meet with the employee at the designated date and time. The department/agency head may designate a committee to hear the employee's answer. The employee may be presented by a person of his choice. The department/agency head must consider the employee's answers to the charges in the proposed adverse action notice. If the employee fails to answer during the notice period, the employee's inaction shall be construed as an answer, and the department/agency head may proceed with the adverse action upon expiration of the notice period.

/ / Chapter 11.308, PR&R, EO96-24 SUSPENSION DURING NOTICE PERIOD

A. An employee against whom adverse action is proposed, must be retained in active duty status during the notice period; however, in an emergency situation, an employee may be immediately suspended during the notice period, under the following conditions:

1. The continued presence of the employee may interfere with the efficient operation of the department/agency, or the health or safety of the employee or others.

2. Suspension is necessary to eliminate the possibility of deliberate damage to equipment, property, or important documents.

3. The employee's absence without authorized leave prevents the issuance of notice of proposed adverse action and the department/agency's attempt to contact the employee was unsuccessful.

B. Suspension under this section is separate adverse action and is appealable to the Commission within 20 days of the effective date of immediate suspension. A copy of the notice of immediate suspension shall be filed with the Civil Service Commission not later than the next working day following the effective date of the suspension.

C. If the Commission sustains the department's action in suspending the employee during the notice period, the number of days of suspension under this section shall be considered part of the final disciplinary penalty and in no case, shall the final days of suspension be more than 30 work days.

/X / Chapter 11.311, PR&R, EO96-24 NOTICE OF FINAL ADVERSE ACTION

A. An employee is entitled to written notice of the department's decision within 10 days after receipt of the employee's answer to the charge(s). The decision shall be made by the department/agency head and shall be delivered to the employee at, or before the time the action will be made effective.

The notice shall be in writing, be dated, state the specific facts found upon which such action is based; inform the employee of his right to appeal to the Commission; and inform the employee of the time limit of 20 days within which an appeal may be submitted as provided in the Personnel Rules and Regulations, Appendix A-CSC-100(c) of the Civil Service Commission Hearing Procedures for Adverse Action Appeals.

B. In the event the appointing authority cannot locate the employee, the Notice of Proposed Adverse Action and/or Notice of Final Adverse Action shall be sent, certified mail, to the employee's last known address.

C. Copies of the final notice of adverse action shall be filed by the department with the Commission not later than the next work day following the effective date of the action. A copy of the final notice shall be filed with the Department of Administration.

CSC-100, PERSONNEL RULES & REGULATIONS, APPENDIX A, EO96-24

/X / A. RIGHT TO APPEAL

1. Any person in the classified service holding a permanent appointment and who is subject to an adverse action by management, except one who is exempted by law from the jurisdiction of the Civil Service Commission, is entitled to appeal an adverse action to the Civil Service Commission. A person who has been appointed to a permanent position and who has satisfactorily completed his probationary period holds a permanent appointment.

2. A contract employee occupying a permanent position in the classified service is entitled to appeal an adverse action to the Civil Service Commission during the term of his contract. Non-renewal of the contract by the government of Guam is not appealable.

/ X/ B. CONTENTS OF APPEAL

An appeal shall be in writing and shall set forth the answer to the charges and the grounds for appeal. An appeal may be amended within 15 days after filing. A person who is the subject of an adverse action and who files an appeal on his own behalf or through a representative is the appellant.

/X / C. TIME LIMIT FOR FILING APPEAL

An appeal must be submitted within 20 calendar days from the effective date of the action.

/X / D. RIGHTS IN PURSUIT OF APPEAL

An appellant shall:

1. Be assured freedom from restraint, interference, coercion, discrimination, or reprisal.
2. Have the right to be accompanied, represented, and advised by a representative.
3. Be assured a reasonable amount of official time to prepare his case if he is on duty status.

NOTE: CHAPTER 11.302d PR&R, EO96-24 DEFINITION OF DAY

Day means calendar days unless otherwise specified.

Please be advised that this department is issuing you a Notice of Final Adverse Action as a result of the allegations set forth in the Notice of Proposed Adverse Action and as set forth herein.

Mr. Espia as employed by GHS/Office of Civil Defense as a Planner IV between August 2000 and September 1, 2007, when he resigned from his position as Planner IV effective September 1, 2007. He then returned to GHS under a re-employment request as a Planner IV effective June 10, 2009 at the Office of Civil Defense. Between 2007-2009, a review of his application shows that he was the president and CEO of an international corporation, AAV International Corporation, and his employment as a manager at Bedrock Construction Materials/Safety 1st Systems, Inc.

The following were set forth in the proposed adverse action personally served on you. You responded orally and in writing to me on April 25, 2022. I have considered your oral and written response on April 25, 2022, and find that the charges against you are supported by the investigation and your oral response to me on April 25, 2022. I find that all charges set forth in this final action are supported by the facts and circumstances set forth herein.

A. On or after February 1, 2022, Homeland Security Advisor (HSA) Samantha Brennan was informed by Planner IV Leo R. Espia that he had previously purchased and/or obtained access to and used a private or personal server (using file sharing or shared drive protocols), including a cloud and web-based server Frantechca (out of California). Mr. Espia admitted to having a new server up and running and to having purchased that server through Frantechca. See **Attachment 1,** which is a WhatsApp thread between Mr. Espia and HSA Brennan; **see thread dated February 1, 2022 at 3:11:36 pm.**

B. Mr. Espia sent an email to Connie Castro and copied HSA Brennan on an email dated February 2, 2022, at 11:41 a.m. This email suggested that a server had gone down since late 2021 and that an IT team was currently helping him to retrieve important files in the server. He further indicated that they were not successful to do what they needed to do remotely in the past few weeks. This email then states, "They now possess the hardware." Accordingly, they will be able to recover the file. He further goes on to state in this email that "they were able to open a new server for us and it has been up and running for the past week or so. They plan to upload recovered files there." This same email indicates his intent to upload documents in the new server. See **Attachment 2.**

C. It was later discovered later that Mr. Espia had researched and bookmarked Buy VM on his work laptop. Buy VM is an alternative brand sold by Frantech Solutions and referenced below. Mr. Espia also improperly had connected his personal lap top to the work network at GHS/OCD and had been forwarding his work emails to his personal yahoo account in February 2022 without permission or consent of HSA Brennan and the Office of Technology's CTO Mr. Frank Lujan.

D. During the administrative investigation when commenced in February 2022, Mr. Espia was discovered to have several personal email accounts. He used several personal accounts to communicate with HSA Brennan during the investigation including several yahoo accounts and a personal Gmail account.

E. Mr. Espia committed an unauthorized breach of the Government of Guam Wide Area Network (GGWAN) by installing a privately owned server (with file sharing protocols or drives) within the system without prior authorization by the agency or the Office of Technology. He improperly added a personal server (using file sharing or a shared drive) to the government network without the express

written approval HSA Brennan and the Chief Technology Officer (CTO) Frank Lujan Jr from the Office of Technology, Government of Guam.

F. Mr. Espia is also the Director of the Emergency Operations Center (EOC).

G. This breach was discovered on or after February 1, 2022, when HSA Brennan inquired with Mr. Espia about a missed deadline concerning the Comprehensive Emergency Management Plan (CEMP).

H. In this conversation, Mr. Espia contributed his delay to a downed server containing the information on the CEMP project. In an attempt to mitigate the situation, HSA Brennan suggested they bring in the Office of Technology (OTECH) for assistance with the server.

I. Mr. Espia then informed HSA Brennan that he had purchased a personal server.

J. After hearing this, HSA Brennan then contacted Chief Technology Officer Frank Lujan to determine whether or not the installation of a privately-owned server was unauthorized and a breach of the GGWAN. Mr. Lujan confirmed this was a serious and unauthorized breach and that the Office of Technology would conduct its own investigation.

K. Based on information shared by Mr. Espia in February 2022 with HSA Brennan, CTO Frank Lujan revoked the access credentials of Mr. Espia on or after February 17, 2022, and exercised its authority pursuant to 5 GCA Chapter 1, Article 12.1, Sections 106(e)-(g) to secure the network perimeter due to cybersecurity breaches and vulnerabilities at GHS/OCD as a result of Mr. Espia's improper conduct while employed at GHS/OCD.

L. Mr. Espia advised HSA Brennan that he gave out two (2) IP addresses out to various persons to access the network/server internally and externally.

M. When CTO Frank Lujan was provided these two IP addresses and advised by HSA Brennan in February 2022 as to Mr. Espia having a personal or private server, he reviewed the IP addresses. He indicated that one IP address provided for internal access to the server and the other one allowed external access. The IP address that allowed for internal access was an open IP and he said there was no firewall to protect against unauthorized access and that anyone could gain access to not only confidential grant information or tactical emergency information but also could get access to the entire GHD/OCD network. The other IP address provided by Mr. Espia to others provided external access to the server. CTO Lujan stated as that was a public IP, it could potentially allow anyone outside of GHS/OCD to gain access to the server and the entire GHS/OCD network. Further, there is the potential for anyone to utilize this unsecured access to the server and network to install malicious programs.

N. On a separate matter, and noted only for prior disciplinary purpose in this action, Mr. Espia was observed making false statements on a zoom meeting with FEMA on January 28, 2022. HSA Brennan joined the zoom meeting late and heard Mr. Espia tell those in the FEMA projects zoom that he had sent HSA Brennan the FY2021 BRIC documents for signature two (2) weeks ago and that he had not received it back. This was a false statement as he had not sent this document to HSA Brennan two weeks as he mentioned. He received a letter of warning for making false statements to FEMA partners and also for making false and misleading statements to those who attended the Emergency Operations Center briefing on February 16, 2022, at 9 am. A letter of reprimand dated February 17, 2022, for

these two (2) incidents was served on him on February 17, 2022. Upon information and belief, he was also removed from his security manager duties prior to 2019 after a complaint was made against him for improperly requested personally identifiable information from federal counterparts.

O. Mr. Espia did not report to work on February 18, 2022. He also failed to comply with HSA Brennan's order to meet with her at her office on February 18, 2022. The order on February 18, 2022, was communicated verbally and in writing by HSA Brennan to Mr. Espia after he failed to report to work on February 18, 2022.

P. Mr. Espia did not answer HSA Brennan's calls so she had an employee call his cell phone. When he answered that employee's call, HSA Brennan spoke with Mr. Espia and directed him to meet with her at 3 pm that afternoon. Mr. Espia was aware of this order but failed to come to work, failed to meet with HSA Brennan on February 18, 2022, and failed to inform her he would not be attending the meeting with her at 3 pm.

Q. Thereafter, Mr. Espia was placed on administrative leave commencing on Monday, February 21, 2022. He has not reported to work since February 17, 2022.

R. HSA Brennan emailed her memo placing Mr. Espia on Administrative Leave to Mr. Espia at his [redacted] email address on February 18, 2022, at 5:19 pm. The body of the email as well as the attached memo advised him he was on administrative leave effective Monday, February 21, 2022. She ordered him to acknowledge receipt of that email, to sign the document, scan and email it to her by Monday, February 21, 2022, at 8:00 am. See **Attachment 3.**

S. On February 25, 2022 at 6:15 pm, HSA Brennan emailed Mr. Espia again and attached the administrative leave memo. She sent this memo to his email address [redacted] and to a new email address from which he had communicated, [redacted]. Despite emailing her about the letter of warning, he failed to answer her order for him to sign and return the administrative leave memo and to acknowledge receipt of her email dated February 18, 2022. See **Attachment 4.**

T. On March 1, 2022, at 6:25 pm, HSA Brennan sent a third email to Mr. Espia, and this time sent this email to three of his personal email accounts, including: [redacted] and [redacted] See **Attachment 5.**

U. The administrative leave memo is attached as Attachment 5. It was emailed to Mr. Espia on February 22, 2022. See **attachment 6** which includes the memo sent to Mr. Espia and the USPS mailing receipt dated February 22, 2022.

V. Despite emailing and mailing the administrative notice, Mr. Espia failed to sign and return the notice until March 03, 2022 via priority mail and also on March 23, 2022 after meeting with investigators Erlinda Blas-Merfalen and Donald San Agustin. See **Attachment** 7. He also refused to answer telephone calls by various persons who attempted personal service of this memo at his residence in February and March 2022. His house is enclosed by a fence around the property with no doorbell.

W. Mr. Espia's failure to acknowledge HSA Brennan's emails and to sign and return the form by the deadline given are considered multiple acts of insubordination and also considered discourteous treatment toward his supervisor.

X. While employed by GHS/OCD, Mr. Espia improperly accessed and used confidential and sensitive government information (to which he had access at GHS/OCD as part of his work duties) from or with a personal/private and web or cloud-based server (Frantech/Buy VM) without the knowledge and consent of HSA Brennan and the Guam Homeland Security / Office of Civil Defense. This conduct was not authorized and was concealed from HSA Brennan by Mr. Espia before February 2022. HSA Brennan was Mr. Espia's supervisor from the end of October 2021 to present.

Y. Mr. Espia breached his duty to maintain security protocols and security information assurance protocols of which he was aware while employed with GHS/OCD. He had been trained in security policies and protocols and he trained others in the office on security protocols between 2013-2018. At one point he was a security manager and liaison as part of his additional related duties.

Z. Mr. Espia failed to ensure the security of the GHS/OCD network and to assure the security of confidential and sensitive government information. He breached this duty and responsibility when he allowed private and remote access to this information and when he purchased a web-based server and installed or hooked up a server to the network without prior clearance and permission.by GHS/OCD. Because he did this without anyone's knowledge at GHS/OCD, he failed to ensure the information was properly protected from cyberattacks, malware and allowed the network to be vulnerable to attack. Although this issue has now been resolved by OTECH, the secretive conduct was a major security breach and was reckless, unethical and criminal. It is unknown if Mr. Espia was providing confidential information to others but that could have occurred as a result of his secretive and unauthorized conduct.

AA. Mr. Espia obtained, used and accessed a private and personal server which he kept in his office. He requested the help of Edison Natividad, currently employed by DPHSS, and who was not employed by GHS or the Guam Homeland Security /Office of Civil Defense, to assist him in fixing the network server. This work was done without the prior knowledge and approval of GHS/OCD, HSA Brennan or the Office of Technology (OTECH).

BB. When this network server /tower became inaccessible and did not work on or about late 2021 or early 2022, such that Mr. Espia could not access information he used for his work-related purposes, including his work relating to grants, he claims he reached out to his friend Edison Natividad at DPHSS to again assist him with this server.

CC. Mr. Espia stated Edison Natividad initially set up this tower and server in his office. He admitted to HSA Brennan that when remote access to resolve the issue did not work that he delivered the "hardware" to the IT person helping him because there was a "no visitor" policy at GHS/OCD.

DD. At no time, however, did Mr. Espia have any discussions with HSA Brennan about any issue relating to a private or personal server before February 1, 2022. He concealed this material information from her about a private or personal server, and his granting remote access to Edison Natividad or to Edison's prior installation of the 2017 server in Mr. Espia's office at GHS/OCD.

EE. Later, in a subsequent interview, Mr. Espia told investigators that he never took the hardware or tower out of his office at GHS/OCD. One of these statements is false as they conflict. Either way, he failed to advise HSA Brennan and the CTO of this improper conduct which violates security protocols and is a cybersecurity breach which Mr. Espia concealed.

FF. When the network server in his office did not work such that, he could not access information for the grant and his work-related duties, Mr. Espia claims he then purchased a web or cloud/based virtual server through Frantechca Solutions.

GG. Mr. Espia made conflicting statements as to the current whereabouts of the network server installed by Edison Natividad. He stated it is still in his office at GHS and is on the top of a metal cabinet, however Edison Natividad was asked to and came to GHS to look into his office to see if he could find the network server. Mr. Natividad was unable to find or locate the network server in his office or in the EOC (Emergency Operations Center). This is another false and inconsistent statement made by Mr. Espia and a further attempt to conceal his misconduct.

HH. Mr. Espia made inconsistent statements as to his purchase of this web/cloud server, including how long he purchased this server. At first he said he purchased it for one year and later he said he purchased it for 2-3 months.

II. Mr. Espia did not mention he purchased anything from Buy VM in his initial interview and admitted to knowing about Buy VM only after he was told that Buy VM was discovered bookmarked and on his work computer. Buy VM is an alternative brand of Frantech Solutions.

JJ. A review of Mr. Espia's office by OTECH revealed he had a personal DELL laptop connected to the network at GHS/OCD between February 2022 to present.

KK. A review of his work email account settings in April 2022 indicated Mr. Espia was also improperly forwarding his work emails, that contain confidential and sensitive information, to his personal yahoo account in February 2022, before this account was disabled by OTECH.

LL. In an interview on April 14, 2022, Mr. Espia admitted in February 2022, before his work email access was disabled on or about February 18, 2022, he accessed his work email from his personal telephone and his personal laptop. He confirmed he forwarded his work emails to his yahoo personal account. He also indicated that he paid for additional storage relating to his work email address and increased the storage from 2 gigabytes to 100 gigabytes.

MM. Mr. Espia did not receive authorization to connect his personal laptop to the GHS/OCD network or to purchase or obtain a personal or private physical server or to purchase a web/cloud based virtual server to upload, download, store or otherwise access confidential and sensitive government information.

NN. Mr. Espia did not obtain authorization to have anyone other than the Office of Technology set up any server or to set up or connect any server to the network at or network at GHS/OCD. He had access at work on a network but no other access was authorized.

OO. Mr. Espia has a personal relationship with Mr. Natividad and the two have had private business dealings relating to personal property. This personal relationship was not disclosed by Mr. Espia to investigators and is a breach of his duties and ethical responsibilities. Mr. Espia did not receive permission to connect any of his work computers to a private server or virtual server, did not receive permission to connect his personal lap top to the network and then to a personal or private server.

These actions are a cybersecurity breaches and violated security information assurance and confidentiality protocols.

PP. Mr. Espia's secret and concealed conduct caused vulnerabilities in the network and were not authorized. Mr. Natividad was not an employee of GHS/OCD and Mr. Espia should not have allowed him remote or other access to any network server /tower, or equipment at GHS/OCD, or which could access confidential information at GHS/OCD, without proper authorization and consent in writing by HSA Brennan and the Office of Technology.

QQ. After his work email was disabled on or about February 18, 2022, Mr. Espia thereafter contacted individuals in an attempt to seek assistance in deleting emails.

RR. As stated above, Buy VM was found on Mr. Espia's work computer at GHS/OCD after it was returned by his wife in March 2022. BUY VM is the alternative brand sold by Frantech Solutions.

Frantech Solutions is a Canadian hosting provider that owns and operates BuyVM.net. The address is: https://frantech.ca/. Frantech Solutions provides storage space and bandwidth. It sells servers and also offers multiple virtual private servers through its **BuyVM website.** Online research shows Frantech Solutions hosted more than 100 malware websites, the 6th most out of any ISP in the world. The company offers services, cloud storage and databases, cloud file systems, virtual private cloud services, applications, platforms and numerous other services.

SS. Mr. Espia made false, misleading and inconsistent statements as to the server(s) when questioned and for the most part attempted to avoid questioning from HSA Brennan and investigators during the period of his administrative leave. At no time did he initially mention BuyVM to HSA Brennan or investigators, yet BUY VM was on his DELL lap top and came up when the computer was put into the docking station. After Mr. Espia realized that the network server was unable to be repaired, he then purchased a web-based server through Frantech. This was all done without the knowledge and consent of GHS/OCD and HSA Brennan. The investigation revealed Frantech is affiliated with Buy VM and that these are foreign companies linked to Canada and China.

TT. Mr. Espia improperly allowed remote access of a network server he used at GHS/OCD by a third party after it was not working without advising HSA Brennan of any issues. He thereafter purchased a web-based server without the permission and consent of HSA Brennan and without advising her of any issues as to the network server, or that he had allowed remote access to sensitive government information.

UU. Neither Mr. Natividad nor Mr. Espia discussed this matter or received the approval from HSA Brennan for any hardware or server to leave GHD/OCD or for an outside person to access or review (whether remotely or in person) any physical or web-based server used at any time to access to confidential and sensitive government information.

VV. Mr. Espia refused to appear before HSA Brennan on February 18, 2022, at 3 pm at her office despite her verbal order to him on his call phone and his acknowledgement of this order on February 18, 2022.

WW. Without the consent of HSA Brennan, Mr. Espia also forwarded all of his work emails at GHS/OCD to his personal yahoo account. This was not discovered by HSA Brennan until on or about April 8, 2022.

XX. Mr. Espia has been improperly forwarding his work emails to his personal yahoo email account at least in February 2022 until his work email address was disabled by OTECH for the period of the administrative investigation. After he refused to meet with HSA Brennan relating to his communications about his purchase of a private server, Mr. Espia reached out to employees at GPA seeking to find the name of someone who could assist him in deleting emails. Mr. Espia did not disclose this to HSA Brennan.

YY. Mr. Espia violated HSA Brennan's verbal order for him to report and meet with her at GHS on Friday, February 18, 2022, at 3 pm. She spoke with him directly on his cell phone. He did not show and did not call her to state he would not comply with her directive.

ZZ. Mr. Espia was thereafter notified and placed on administrative leave effective Monday, February 21, 2022.

AAA. Mr. Espia's work email was disabled February 17, 2022.

BBB. HSA Brennan emailed and communicated the administrative leave order to Mr. Espia to his work and personal emails and attempted delivery at his residence, but Mr. Espia did not answer his calls or emails or initially accept personal delivery of the administrative leave and thus it was also mailed to him. At some point after he was placed on administrative leave, he thereafter left for the Philippines with his wife without prior approval from HAS Brennan. He has not reported to work since the end of his administrative leave.

CCC. On and after February 1, 2022, when HSA Brennan was inquiring about Leo Espia's duties and responsibilities relating to an outstanding FEMA grant, Mr. Espia advised HSA Brennan about a "server" having gone down. He later referred to his having obtained a personal or private server.

DDD. Mr. Espia did not communicate with or obtain authorization from HSA Brennan to repair any server or remove any server, hardware or equipment, which allowed access to confidential or sensitive government information, from the office of Guam Homeland Security / Office of Civil Defense. Mr. Espia did not advise or obtain permission from HSA Brennan to allow any person outside of the Guam Homeland Security/Office of Civil Defense to review or fix any issues with any server (personal or private which was used to access or store any government information relating to Guam Homeland Security/Office of Civil Defense) at any time.

EEE. Mr. Espia communicated to HSA Brennan that he was unable to complete the CEMP project because the "server" went down in late 2021. On February 1, 2022, Mr. Espia advised HSA Brennan that he had purchased a personal server for use with the CEMP project. HSA Brennan was Mr. Espia's direct supervisor from the last week of October 2021 through the present date.

FFF. Mr. Espia concealed his having, owning or accessing a personal or private server with government information from GHS/OCD, as well as his purchase of, use and/or access to a web-based server to access and store confidential and sensitive government information relating to GHS/OCD,

from HSA Brennan prior to February 2022. Mr. Espia disclosed an issue with a server only in an attempt to explain why he was not timely in responding to HSA Brennan's grant inquiries. His excuse was that the server went down, and after further inquiry by HSA Brennan on and after February 1, 2022, HSA Brennan was made aware that there was a private or personal server Mr. Espia was using to access confidential or sensitive government information without HSA Brennan's knowledge and authorization. This conduct by Mr. Espia breached his duties and responsibilities, the code of ethics and breached security protocols known by Mr. Espia, and is criminal, unbecoming and notoriously disgraceful.

GGG. Mr. Espia abused his position of trust and authority and misused his office, government equipment and allowed improper access to DHS/OCD information outside of the department in violation of security protocols. He failed to obtain authorization for private and web/cloud servers and to ensure the information was properly protected. These violations have since been corrected by GHS/OCD, with the help of OTECH, to ensure the protection of government and sensitive information. Mr. Espia has attempted to avoid questioning and when questioned between February to present, has provided inconsistent and false statements to investigators Erlinda Blas-Merfalen and Donald San Agustin.

HHH. Mr. Espia failed to indicate to HSA Brennan at any time before February 1, 2022, as to any information that he had used or obtained access to a personal, private and web-based server, including but not limited to, Frantech or Buy VM or other server. He improperly accessed sensitive government information with a private, personal or web-based cloud/sever on and after February 1, 2022, (and most likely for months in advance of February 2022) without HSA Brennan's knowledge and approval at any time since she was appointed the head of the agency on or about the last week of October 2021

III. Mr. Espia did not advise HSA Brennan at any time until after February 1, 2022, that he provided a private server or any hardware for review by a third person not working for the department for review; namely Edison Natividad. This individual was not employed by the department.

JJJ. HSA Brennan was not advised by Mr. Espia of any need or request to provide government equipment or any network server or hardware (whether personal or private) which enabled Mr. Espia to access confidential and sensitive government information, for review by anyone outside of the Guam Homeland Security / Office of Civil Defense, especially a person who was not an employee of the department and was not under contract to review or assist with any network or IT issues. Mr. Espia breached his duties of confidentiality and breached security protocols of which he was aware as he had previously served as security manager and conducted security training within the department.

KKK. The administrative investigation revealed that Mr. Espia, between February 1-17, 2022, if not before, was forwarding his government departmental emails to his personal yahoo account prior to his work email access being disabled. He concealed this misconduct from HSA Brennan. Forwarding government emails from the department to his personal email account is a breach of his security training, security protocols of which he was trained and was aware, and a breach of his ethical and work duties and responsibilities. He was not authorized to forward these emails to his personal account.

Based on the above information previously set forth in the proposed adverse action and the documents attached to this action, as well as the information from the administrative investigation, I find you violated each of the following charges set forth below. Your oral and written response to me on April 25, 2022, support the taking of adverse action against you as well. You orally admitted your misconduct to me on April 25, 2022 and that you took action without my knowledge and consent.

1) **9 GCA § 52.30.** Unsworn Falsifications; Defined & Punished. A person is guilty of a **misdemeanor** if, with *intent to mislead a public servant in performing his official function*, he **makes, submits or uses**: (a) any *written false statement of his own which he does not then believe to be true*; or (b) any physical object, exhibit, writing or drawing which he knows to be either false or not what it purports to be in the circumstances in which it is made, submitted or used.

Mr. Espia made false statements in his written communications to HSA Brennan and to others that were discovered on or after February 1, 2022. These communications include his WhatsApp communications as to the personal or private server, his purchase of a personal server, and his emails to others.

2) **9 GCA § 46.25.** Tampering With Records to Deceive or Conceal; Defined & Punished. A person commits a **misdemeanor** if, knowing that he has **no privilege to do so,** he **falsifies**, destroys, removes or conceals **any writing or record, with intent to deceive or injure anyone or to conceal any wrongdoing.**

Mr. Espia made false statements in his written communications to HSA Brennan and to others that were discovered on or after February 1, 2022. These communications include his WhatsApp communications as to the personal or private server, his purchase of a personal or private server, his emails to others.

3) **9 GCA § 49.90 (Official Misconduct);** Defined & Punished. A public servant commits a misdemeanor if, **with intent to benefit himself** or another person or to harm another person or to deprive another person of a benefit; (a) **he commits an act relating to his office but constituting an unauthorized exercise of his official functions, knowing that such act is unauthorized**; or (b) he knowingly refrains from performing a duty which is imposed upon him by law or is clearly inherent in the nature of his office.

Mr. Espia benefited himself by improperly obtaining and using confidential information and improperly accessing sensitive government information for his personal or private use. This is implied by his secretive conduct and his blatant disregard for the security procedures and protocols, by bringing in a friend to assist him with his own personal services, by his attaching his personal lap top to the network, his failure to report to work and his numerous inconsistent statements.

He committed multiple acts relating to his office that were not authorized and he knew all such acts were unauthorized.

These breaches would not have been discovered had the network server not gone done and had HSA Brennan not inquired as to why he failed to meet grant deadlines.

4) DOA, "PERSONNEL RULES & REGULATIONS": CHAPTER 11, SECTION 11.402 - "RANGE OF PENALTIES FOR STATED OFFENSES":

NATURE OF OFFENSE: CONDUCT

A. Criminal, dishonest, infamous and notoriously disgraceful conduct adversely affecting the employee/employer relationship (on duty or off duty), making false, inaccurate and misleading statements

See all facts and circumstances above and below and as attached to support all charges, including criminal conduct, dishonest, notoriously disgraceful conduct (on duty or off duty), and his making false, inaccurate and misleading statements to investigators and his attempts to conceal his misconduct at work and outside of work (improper conduct relating to forwarding of his government email to his personal yahoo account without authorization and his use and payment of a private or virtual server which he used to upload and/or access or keep sensitive and confidential government emails and information without the knowledge and authorization of HSA Brennan. He also improperly used his personal lap top and had this laptop hooked up to the government server in his office as discovered on inspection by OTECH.

B. Falsification, misstatement or concealment of material fact in connection with any official record – see facts and circumstances set forth herein regarding employee's false statements, his dishonesty and tampering with government records.

C. False testimony in an inquiry or investigation – see all facts and circumstances set forth herein including his false and inconsistent statements to investigators as to his purchase and use of a private server.

5) DOA PR&R Chapter 11 (see page 2 of this action for same charges) **

B. Refusal or failure to perform prescribed duties and responsibilities

C. Insubordination (refusal to attend meeting with Director February 18, 2022 and answer emails and orders from Director).

F. Unauthorized absences (February 18, 2022)

H. Discourteous treatment to the public or other employees.

J. Misuse or theft of government property (misuse of official and confidential information, government email (sensitive but non classified information), misuse of his government office and position, and government equipment).

O. Other misconduct not specifically listed [improperly disclosing confidential or government information without authorization, criminal conduct (official misconduct, tampering with records, unethical conduct; notoriously disgraceful conduct (on duty or off duty) adversely affecting employer/employee relationship, dishonest conduct, making false and misleading statements to investigators, attempt to conceal misconduct, and discourteous and disrespectful conduct. Violation of Chapter 3 DOA PR&R Code of Conduct.

All facts and circumstances set forth herein and as attached support violations of the above, including Mr. Espia's insubordinate conduct by failing to appear at the meeting on February 18, 2022, his failure to answer emails and calls and to sign, scan and email back the administrative leave form. He failed to perform his work duties and responsibilities on February 18, 2022 and was placed on unauthorized leave.

He was discourteous to HSA Brennan by failing to comply with her orders but also by concealing the private/personal server he has obtained as well as his subsequent conduct in getting a web/cloud based server up and running through Frantech/Buy VM without her knowledge and his allowing other persons to remotely access this confidential local and federal government information concerning grants and other work related information to which he had access as a result of his position of trust and duties at GHS/OCD.

He abused his position and allowed the misuse of this information for his personal gain. He also compromised the department's network and breached cybersecurity protocols of which he was aware.

He failed to comply with necessary security protocols to assure the confidentiality of the information to which he had access. He also attached his personal server and personal laptop to the network as well as a cloud based server. Additionally, he ensured all incoming emails to his work as well as his emails were forwarded to his personal email account without permission and prior approval.

Instead of advising GHS/OCD, he engaged a personal friend to assist him with fixing a network server/tower in his office and thereafter consulted that person to fix the server when it went down, although Mr Edison Natividad was not employed by GHS/OCD.

After his work email access was disabled, Mr. Espia then reached out to find someone to assist him with information as to how to delete emails.

6) **4 GCA § 15203. Confidential Information**. No employee shall disclose information which is considered a private document by existing law, and which the employee acquires in the course of official duties, or use the information for personal gain or for the benefit of someone else.

Mr. Espia violated this provision by forwarding all incoming work mail to him at GHS/OCD to his personal yahoo account and his allowing confidential and written communications, including sensitive federal information and grant information and other documents to be accessed remotely by others and by himself via an unknown and unsecure person/private file-sharing protocol (FTP)/server and also by storing or accessing this information via a web or cloud based server through Frantech Solulions and Buy VM without the knowledge and consent of HSA Brennan and the Chief Technology Officer (CTO) Mr. Lujan.

7) **3.000 ETHICAL CONDUCT AND RESPONSIBILITIES OF GOVERNMENT EMPLOYEES**

A. Public service is a public trust. Employees are expected to be loyal to the U.S. Constitution, the Organic Act of Guam, and to perform their duties and responsibilities ethically and in accordance with laws.

C. **Employees shall not engage in financial transactions using confidential or non-public government information or allow the improper use of such information to further any private interest.**

G. **Employees shall not use public office for private gain.**

H. Employees shall protect and conserve public property and shall not use it for other than authorized activities.

N. Employees shall be courteous to other employees and respect supervisory authority.

You violated the above ethical provisions by your failure to advise your supervisor of your conduct as set forth in this action and by failing to meet with her as ordered on February 18, 2022, at 3 pm as ordered. You improperly used confidential information for your private gain and personal purposes. You failed to protect and conserve public property and you used government property (your position, your office and work computers and improperly used your office, position and your work-related access to sensitive local and federal information to further your private interests. See all facts and circumstances set forth and as attached to support each and all charges in this action to avoid duplication.

You were personally served with the Notice of Proposed Adverse Action by OAG investigator Donald San Agustin on April 15, 2022. You had ten calendar days after receipt to request to meet with me if you wanted to orally respond to the charges. On Friday, April 22, 2022, you requested to meet with me on the tenth day, April 25, 2022. We met at 1030 am as agreed by you and the meeting was less than one hour. Although you have requested to be on sick leave and been on approved sick leave, you will be paid one hour of administrative leave for the period of your response. At our meeting on April 25, 2022, you provided me with documents including your written response dated April 25, 2022.

I have considered your oral and written responses to me yesterday, April 25, 2022.

I made this decision today, April 26, 2022, after considering both your oral and written response submitted yesterday, April 25, 2022, the last day for you to respond. I have also considered the information in this investigation. You admitted to forwarding your work emails to your private yahoo email and to accessing Buy VM and Frantech. Based on the seriousness of the charges against you, including your dishonest, insubordinate, unethical, secretive and criminal conduct, I find that the action taken on page 1 is appropriate.

In your oral response yesterday, April 25, 2022, you admitted you took action without me. You also admitted to your personal relationship with Edison Natividad and that you spoke with him twice between February 18, 2022 and this month, April 2022. You advised that you have co-signed a loan for him and have met at each other's homes in addition to going to church together. You also indicated you spoke with someone face to face at church while you were on sick leave that told you about "apparent fixes done on our computers two weeks ago." You refused to identify the name of that person and said although you met that person at church in April 2022, you did not know whether the person was male or female, and you could not remember the name of the person. You admitted to me that you communicated with persons at GHS/OCD while you were on administrative leave. This communication was in violation of the administrative leave orders, which is just another example of your insubordinate conduct. You refused to meet with me to discuss the matter of your private personal server on February 18, 2022, as ordered.

Your written response to me dated April 25, 2022, failed to take any responsibility for any of the charges against you. You clearly were not remorseful nor apologetic, nor did you apologize or ask for any leniency.

Guam Homeland Security/Office of Civil Defense is the epitome of the highest standards as we work with our federal counterparts and any form of impropriety or the illusion of the truth is unacceptable. Your conduct was stated above (and as attached) is reckless, unethical, unprofessional, dishonest and notoriously disgraceful. It is also criminal. You continued to conceal your dishonest, unethical and criminal conduct and after being placed on administrative leave continued to contact persons without authorization and contacted a third person to find out how to delete emails. You abused your position of trust and misused your position and office by failing to ensure the confidentiality of security of sensitive government information and by allowing access by others to the GHS server and network without security and without my knowledge or consent. Had this server now gone down, and I had not inquired as to why you were late responding to a grant, your improper and secretive conduct may not have been discovered. You took action without knowledge and consent as stated in this action, including obtaining and installing a private server without protecting the network and thereafter obtaining access to and purchasing a cloud-based server without my knowledge and consent.

OTECH confirmed the seriousness of the cybersecurity threat and breach. There was no reason for you to engage in this conduct other than for your own personal gain and purposes. Your unethical, unbecoming and criminal conduct put the security of confidential and sensitive information at risk. Fortunately, your recent conduct and your attempts to conceal your misconduct came to light and have now been corrected. Your dishonest, unethical, insubordinate and criminal conduct is also notoriously disgraceful and adversely affects the employer/employee relationship. You cannot be trusted to perform your job duties and responsibilities ethically and honestly. The efficiency of the service requires nothing short of your dismissal.

You have twenty (20) calendar days from service of this action to file an appeal of this action to the Civil Service Commission.

Name of Department/Agency Head: **SAMANTHA J. BRENNAN** **HOMELAND SECURITY ADVISOR** **GUAM HOMELAND SECURITY / OFFICE OF CIVIL DEFENSE**	**Signature of Department/Agency Head:** **Date:** April 26, 2022 **Time:** 1158 am

Signature of Employee being served:	**Date:**	**Time:**
	April 26, 2022	1:34 pm

I hereby certify that a copy of this notice was served on the subject on the 26TH day of APRIL, 2022.

/ V **SERVED PERSONALLY**
/ / **REGISTERED MAIL**
/ / **COPY LEFT AT LAST KNOWN ADDRESS**

Name of Person Serving Action: AGI Donald San Agustin
Signature of Person Serving Action:
Date Served: 04/26/22
SEE ATTACHMENTS 1-7 CONSISTING OF 17 PAGES

Enclosure 6 (Response to Notice of Proposed Adverse Action)

GUAM HOMELAND SECURITY/OFFICE OF CIVIL DEFENSE
Inasiguran I Tano' Guahan/Ufisinan Difensia Sibet
221-B Chalan Palasyo, Agana Heights, Guam 96910
Tel: (671) 475-9600 / Fax: (671) 477-3727
Website: www.ghs.guam.gov

Lourdes A. Leon Guerrero
Governor

Joshua F. Tenorio
Lt. Governor

Samantha J. Brennan
Homeland Security Advisor

Charles V. Esteves
Administrator

April 25, 2022

Ms. Samantha J. Brennan
Homeland Security Advisor
Guam Homeland Security/Office of Civil Defense
221-B Chalan Palasyo
Agana Heights, Guam 96910

Subject: Response to the Proposed Notice for Adverse Action

Hafa Adai Ms. Brennan:

This has reference to the Notice of Proposed Adverse Action dated April 15, 2022. Please accept this letter as my response. This written response will be supported by an additional verbal response during our meeting today, 25 Apr 2022.

Background –

- During the first section's program/project briefing with the new Homeland Security Advisor (HSA), Ms. Samantha Brennan, who assumed her roles and responsibilities on 29 Oct 2022, I emphasized the top two (2) challenges the Guam Homeland Security/Office of Civil Defense (GHS/OCD) as follows:
    - Morale and welfare of GHS/OCD employees – Increments not processed for several employees, etc. In fact, my three (3) consecutive increments have not been processed until this time.
    - Information Technology (IT) capability of GHS/OCD – No IT/Cybersecurity Officer on board, issues on old computers, network issues, etc. I was very serious when I brought this up. We badly need help and the GHS/OCD workforce continues to survive day by day as we strive hard to accomplish our tasks. Nothing has been done except for the apparent fixes done on our computers two weeks ago which were obviously triggered by the administrative case against me.
- Conflict situation during my earlier meeting with the HSA emanating from her discriminatory actions relative to my being a senior citizen that I need to retire in one year and that I need to turn over what I do.
    - Related harassment and discriminatory actions towards two (2) other employees of Filipino ethnicity followed. These were subjects of multiple Incident Reports submitted via the GHS/OCD Administrative Services Officer (ASO)/Equal

Employment Opportunity (EEO) Counselor. I am not sure if there are other cases. My ethnic background is Filipino.

- The HSA's misinterpretation that I was providing misinformation and inciting the Response Activity Coordinators/Emergency Support Function Coordinators (RAC/ESFC) to question the decision on changes to the Emergency Operations Center (EOC) activation during the 0900 EOC Briefing on Wednesday, 16 Feb 2022.
- Relevant Letter of Warning was served to me immediately by the HSA at 1100 on the following day, Thursday, 17 Feb 2022.
- My government email, leo.espia@ghs.guam.gov was disabled at around 1345 on the same day, 17 Feb 2022. It was confirmed by the Chief Technology Officer (CTO), Office of Technology (OTech), Mr. Frank Lujan, that this was directed by the HSA.
- When things kicked in, I became very ill that night, requested to go on Sick Leave via email at around 0712 and 0910 on Friday, 18 Feb 2022, and went to see a doctor that afternoon. A medical certificate was provided via email later. I was unable to meet with the HSA at 1400 that day due to my medical condition and my medical appointment scheduled that afternoon. I left the clinic that afternoon close to 1600. The Time Sheet for that pay period and the Sick Leave Form were emailed later and copies were sent via US Postal Services, Tracking Number 9405 5036 9930 0177 8591 27.
- A law enforcement officer, apparently directed by the HSA, went to the clinic where I was treated in the afternoon of my follow-up medical checkup on Monday, 21 Feb 2022, apparently to obtain my health information. I was concerned about my health information. My medical condition worsened and necessitated for me to be on Sick Leave until referred off-island for medical treatment, further tests, and a second opinion for a short period.

Some entries in this response are estimates. I don't have references with me because I don't have access to my system, email, etc.

- The HSA directed the Director of the Office of Technology to disable my GHS/OCD official email and I don't have access to my email until this time.
- The HSA has prohibited me from doing the following until this time:
    - I am prohibited from doing work.
    - I am prohibited from entering the GHS/OCD facility. I was directed to surrender my facility access badge.
    - I am prohibited from communicating in any form with the GHS/OCD staff and stakeholders which will include the RAC/ESF Coordinators and Federal/DOD partners.
    - I was directed to surrender my laptop computers, etc.
- The HSA has prohibited the GHS/OCD staff from communicating with me until this time.

Refusal or failure to perform prescribed duties and responsibilities –

The hostile environment that we have currently in our workplace may have led to spontaneous inaccurate declarations most especially in text messages. The HSA's shouting, and to some extent harassing, at our employees in front of other employees, employing most often "negative reinforcements", etc., may have caused the employees to just keep quiet and make solutions to the office problems on our own.

On my end, when I say that "we got it", it means we have it or we can re-create things in a short period with the tools and the data in place. This is shown by our team's performance in previous collaborations and our large plans, such as Guam Hazard Mitigation Plan, Guam Comprehensive Emergency Management Plan, Guam Catastrophic Plan, etc.

- **On GHS/OCD organization-wise -**

GHS/OCD are two organizations rolled into one. The Office of Homeland Security (OHS) was created by an Executive Order (EO) and the Office of Civil Defense (OCD) was established by the Organic Act. It has been customary for us to take up everything concerning emergency management with the OCD Administrator.

Our OCD Administrator has been on military leave for about two (2) years now. In his absence, two (2) Acting OCD Administrator has been designated. Unfortunately, since November 2021, no one was designated.

During my discussion with the HSA late last year, she mentioned to me that she will designate somebody by Jan 2022. However, until now, no one was designated. This affected how we take care of problems in the office.

- **On the Guam Comprehensive Management Plan (GCEMP) -**

The maintenance of the Guam Comprehensive Emergency Management Plan (GCEMP) is the responsibility of the OCD Administrator. I assist him to coordinate this but this task is "all hands on deck".

I am not involved in the routine grant conference calls not until a few months ago. We are on it but resources and priorities have deviated to COVID-19 response. It was impossible to assemble and meet with our task forces and working group due to COVID-19 restrictions, the spike in numbers that happened in September 2021 and January 2022.

We were on it but resources were not cooperative and priorities have deviated to COVID-19 response.

I was discussing this task with FEMA as we finalize the plan to have everything in place way before the FEMA grants monitoring visit scheduled for 21-25 Mar 2022. However, my email was disabled and I am currently in this situation

Insubordination (refusal to attend meeting with Director February 18, 2022, and answer emails and orders from Director). -

The scheduled meeting with the HSA at 1400 on Friday, 18 Feb 2022, announced at 1100 that day was already in conflict with my medical appointment that afternoon. It was mentioned during the phone call at 1100. My business with the clinic was concluded close to 1600. Most importantly, my medical condition that day incapacitated me from going anywhere except home to rest. Furthermore, I was on sick leave during that day.

My government email was disabled without warning and I don't have access to it until this time. This is the first time that this happened to me in the past 20 years. As such, I was not prepared for what to do. I was forced to try to use my yahoo email which I don't use often, which is full of junk emails, email promotions, unwanted subscriptions, etc., more or less, a hundred of them per day depending on the day of the week. I tried another Yahoo email but I had indications that my Yahoo emails (could be those coming from Leo Espia) are blocked off or not going through. I also tried my Gmail email, hoping that Gmail will go through because the ghs.guam.gov email is running on the Google platform, to no avail.

Since the HSA remove me from the GHS/OCD WhatsApp chat and Command Staff chat including the MRFC chat, WhatsApp is no longer our primary means of communication. Also, since my cellular phone, which has no use for me anymore, has been temporarily detached from me as part of the doctor's advice, communicating via the US Postal Service has been the best way of communicating. During the pandemic, our village mailbox became our primary mailbox instead of our USPS Tamuning mailbox. It is very seldom that we check our Tamuning mailbox. This is the reason why the Administrative Leave was received late.

Unauthorized absences (February 18, 2022). –

I requested Sick Leave on 18 Feb 2022 via an email I sent early that day. The email was sent to the HSA copy furnished the GHS/OCD Administrative Services Officer (ASO) and the Administrative assistant (AA). A supporting medical certificate was provided immediately after seeing my doctor. Apparently, records show that the day I requested Sick Leave on 18 Feb 2022, I was not paid.

Subsequent requests for Sick Leave have been substantiated by medical certificates including medical referral for off-island. All the required documents have been submitted to the HSA copy furnished by the GHS/OCD ASO.

Discourteous treatment of the public or other employees. –

and

Misuse or theft of government property misuse of official and confidential information, government email (sensitive but unclassified information), misuse of his government office and position, and government equipment). -

and

Other misconduct not specifically listed [improperly disclosing confidential or government information without authorization, criminal conduct (official misconduct, tampering with records, unethical conduct; notoriously disgraceful conduct (on duty or off duty) adversely affecting employer/employee relationship, dishonest conduct, making false and misleading statements to investigators, attempt to conceal misconduct, and discourteous and disrespectful conduct. Violation of Chapter 3 DOA PP&R Code of Conduct. -

- **On the alleged personally owned server –**

The subject server is not personally owned. No part of the server belongs to me.

It was set up by a GHS/OCD employee sometime in 2017 alongside the setting up of the Mariana Regional Fusion Center (MRFC) Unclassified Workstation, Server, and Network Project which was started by the Guam Police Department's (GPD) SGT Jesse P. Rodriguez and supervised by the MRFC Deputy Director COL Joseph Leon Guerrero, a Deputy Marshal from the Judiciary of Guam. Since it was set up, it was never taken out of the GHS/OCD facility nor serviced by anyone outside of our agency.

My request during that time was, if possible, to set up an FTP site for the sole purposes as follows:

- To address NOAA requirements relative to our National Tsunami Hazard Mitigation Program (NTHMP) Grant. NOAA Data Publication Sharing Directive for NOAA Grants, Cooperative Agreements, and Contracts states that access to grant/contract-produced data is enabled. This was a requirement since our FY2017 NTHMP Grant and the NeoWave modeling of Guam's coastal communities but the University of Hawaii started with our FY2018 NTHMP Grant. The NeoWave Modeling Project continued until our FY2021 NTHMP Grant. Relevant funds are also being applied for in our FY2022 NTHMP Grant.
- To address FEMA requirements on the Whole Community Planning as indicated in the Community Planning Guide (CPG) 101 and the various Emergency Management Performance Grant (EMPG) work plans. The FTP site will serve as a plan and data-sharing site. Previously, we were using the Yahoo Group platform. Currently, everyone is doing file sharing via Google Docs.

- To share conference, workshop, or meeting materials with specific stakeholders/ participants including our Response Activity Coordinators (RAC)/Emergency Support Function (ESF) Coordinators, and military and federal partners.

This request for an FTP site was triggered by the failure in the procurement of a server and accessories funded by our FY2017 NTHMP Grant. Despite the repeated coordination meetings in the Office of Technology (OTech) with Chief Information Technology (CTO), Mr. Frank Lujan, and his Deputy, Mr. Joseph Manibusan, and complying with their requirements including changes in specifications, we lost the grant funds. The General Services Administration (GSA) was not able to issue the Purchase Order due to the inaction of OTech until the grant's performance period ended. This has reference to GSA Requisition Number Q182300-193.

The server in question is a tower of an old desktop computer pulled from the Emergency Operations Center (EOC) when the desktop computers were upgraded. The remaining two (2) of the old desktop computers are still the EOC sitting as junks.

GHS/OCD management and key staff are aware of this desktop server. It is not a secret as alleged and it was never been used for personal gain. In fact, GHS/OCD procured a dedicated IP address from GTA for its use. Our OCD Administrator, Mr. Charles Esteves, who is currently on military leave, is aware of the server and has downloaded emergency management plans due to their file sizes. The URLs are announced during our conference, workshops, and meetings, normally indicated in the second to the last slide of the slide deck, to lead the participants or planning partners where they can download the presentations and plans for a limited period.

Unfortunately, it is temporarily set up in my office due to the lack of space in the Server Room and the EOC. I don't have a desktop computer and I try to live each day with my unreliable old Dell laptop. My desktop computer was re-issued to my Planner I, Ms. Yoni Towai. Since she came on board, she was not issued a desktop computer.

Our OCD Administrator was trying to obtain the Shareware before he went on military leave to help us with our problem. I will check with Admin where they are at with this procurement.

During the use of this server which is known to key GHS/OCD staff including OTech as they are representing Emergency Support Function (ESF) 2 during task force and workgroup meetings, there was no action that I or my team performed that is considered improper obtaining and using confidential information and improper accessing sensitive information for my/our personal or private use. Likewise, no information was ever shared with unauthorized agencies/individuals and it was never used on purposes outside of the aforementioned sole purposes.

- **On the procurement of off-island servers -**

I researched immediate solutions or options for servers. In doing so, I procured certain accounts for the trial run. The purpose of which is to recommend to GHS/OCD management the most viable options out there. The accounts I procured are:

  - AppSumo

  I procured an account in AppSumo and was refunded when it was found out that it will not serve the purpose. The account was never used and no personal or government data was ever uploaded and/or shared.

  - FranTech/BuyVM

  I procured an account in BuyVM but the receipt was issued by FranTech for about $19.00+ for trial. It was found out that it will not safely serve its purpose. This transaction cannot be refunded. The account was never used and no personal or government data was ever uploaded and/or shared.

- **On the forwarding my email -**

The auto-forwarding was my only solution as a non-IT person to achieve emails. I set this up way before 01 Feb 2022. This is triggered by the lack of a repository of old government emails beyond 5GB or 10GB of storage and my never-ending deleting of old emails to accommodate incoming emails. There were numerous times when I cannot produce the documents the auditors or the Federal grant monitors are looking for because the emails have been deleted. There were times that I have to re-create project files from over a decade ago like the EOC Facility Expansion Project and All-Hazards Alert Warning System (AHAWS) Project because they are nowhere to be found. Most often, due to the urgent need to receive the incoming emails, I simply delete blindly my emails from Jan to Dec of a specific year and quickly empty the trash. As an example, since we are mandated to retain the grant documents until 36 months after the grant end date, the email approval of requests (aside from the approval letter, some approval is indicated in a plain email discussion) cannot be produced.

The forwarding is to my personal email opened purposely for achieving ONLY. No one has access to it and none of the emails therein was forwarded to anybody. In fact, I do not open that email until this past month to see if my government email is already re-activated.

Unfortunately, GHS/OCD has no IT policy in place. How I wish OTech is conducting related training or outreach as well as refresher training on IT policies.

During the forwarding of my emails for archiving purposes, there was no further action that I performed that is considered improper obtaining and using confidential information and improper accessing sensitive information for my/our personal or private use. Everything was

for government use and purposes only. Likewise, no information from this forwarded email was ever shared with unauthorized agencies/individuals and it was never used on purposes other than archiving for government use only. My emails were forwarded to myself only, no one else, and it stops there.

I respectfully request/recommend the following:

- For OTech to host GHS/OCD server for the aforementioned purposes,
- Pursue another procurement of GHS/OCD server,
- Pursue procurement of Shareware as directed earlier by the OCD Administrator,
- For GHS/OCD and OTech to provide the tool to archive emails so that employees will not keep on deleting emails, and
- To solicit support/contract out the University of Guam's (UOG) Global Learning Engagement (GLE).

I respectfully assert my Garrity rights in this administrative process.

Should you have any questions, I will make myself available. However, I am currently on Sick Leave. In the meantime, you can email me at [redacted]

Respectfully,

Leo Rustum J. Espia

Enclosures

Copy Furnished: Administrative Services Officer/EEO Counselor, GHS/OCD