MEMORANDUM OF AGREEMENT
BETWEEN THE
GODDARD SPACE FLIGHT CENTER
AND THE GODDARD ENGINEERS, SCIENTISTS, AND TECHNICIANS ASSOCIATION
AND AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES
INFORMATION TECHNOLOGY (IT) SECURITY ANTI-PHISHING TRAINING

PARTIES

The parties to this Memorandum of Agreement (MoA) are the Goddard Space Flight Center, (hereafter, "GSFC", "Center" or "Management"), Goddard Engineers, Scientists, and Technicians Association (GESTA) and American Federation of Government Employees (AFGE) (hereafter, "Labor").

PURPOSE

Phishing is a form of social engineering designed to trick a person into supplying personal or proprietary information for the purpose of fraud or identity theft. Due to an increase in phishing incidents involving NASA end-users, the agency's Office of the Chief Information Officer (OCIO) will be requiring mandatory training for "recurring clickers" to increase awareness from an Information Technology (IT) Security perspective about phishing attacks.

The primary objective of this initiative is to educate and reinforce the importance of appropriately responding to phishing attempts whether real or potential. This MoA covers the terms and conditions under which this objective will be implemented at GSFC.

This MoA is applicable to AFGE and GESTA covered bargaining unit employees.

This MoA has no effect on any other agreement(s) that may exist between Management and Labor.

AGREEMENT

Labor and Management agree to the following:

(1) All IT Security training as mandated by the Center shall include an emphasis on the following:

(a) Definition of phishing, and its various forms, e.g., spear phishing, phone phishing, etc.

(b) Explanation of the methods used to conduct a phishing attack, and what motivates cybercriminals.

(c) The impact of phishing to NASA and employees, personally.

(d) How to recognize a phishing email.

(e) Best practices to avoid in becoming a victim.

(f) How to respond to a phishing attempt.

(2) Standard Agency Tool sets, which consist of e-mail filters, spam filters, etc., will be utilized to help alleviate the presence of phishing scams. The Center will mitigate phishing attempts through automated tools; however, ultimately combating phishing requires end user awareness, preventative action, and training.

The Agency's anti-phishing engagement program will also include periodically sending "fake" phishing e-mails to all NASA employees, which shall be limited to no more than per two (2) per month and no more than twelve (12) per calendar year. When a NASA employee clicks on any link inside such e-mails, which the user is not supposed to do, the link will actually lead to a NASA website. Should the user click on this link, the identity of the user will be recorded to a database which contains the date and time-stamp of the fake e-mail and the identity of the user. This information shall be verifiable so an electronic data trail is available in the event that there is any dispute. The User will get a notice and will be **"invited"** to attend phishing training in order to improve his/her skills.

A "recurring-clicker is defined as an employee who enters data on a website provided as part of a phishing exercise, clicks on a web link embedded in a phishing test email, or provides data in response to a test email sent during an OCIO phishing exercise two times (i.e., two separate test emails) within a nine (9) timeframe.

(3) In addition and subsequent to all of the terms above, "recurring-clickers" will be required to attend an instructional training session, to be loaded into their SATERN training profile. This training shall serve as an informative and educational purpose, and in and of itself is not disciplinary in nature. Additionally:

(a) The training for "recurring-clickers" is designed for approximately 60 minutes, but shall not exceed 90 minutes.
(b) Management shall provide at least three (3) training opportunities within a calendar year (and at least one training session shall be available every four months in the calendar year), for the employees at issue to complete the training, and shall communicate each of these opportunities to employees via email notification as well as via their SATERN training profile. The training shall be capable of being conducted face-to-face, and/or via videoconference for the different worksite locations (i.e., Greenbelt, Wallops Flight Facility, GISS, IV&V, etc.).
(c) If the additional instructional training is required as described above, then it will normally be completed by the employee within six (6) months of the SATERN training profile notification, unless there are either circumstances beyond control of the employee, such as the date of the next available training is beyond six (6) months, or the employee's Supervisor approves more time due to work requirements, or there are other mitigating circumstances. Employees shall not be disciplined for not being able to take the required training provided that they make reasonable efforts to take the

required training, e.g., an emergency occurs on or about the date of their required training and they schedule the training on the next available date.

(d) While most employees will take the training at their worksite, employees shall not be required to travel outside the local commuting area for this training. Employees who normally telework outside of the Center or facility commuting area on a regular basis shall be offered the opportunity connect to the required training remotely from their work stations by WebEx, Adobe Connect, or other similar means.

(4) The parties agree that this policy is not intended to bait employees into sudden non-compliance with existing IT Security policy or otherwise entrap employees. Rather, the intent is to test employee responses to a phishing scenario in a manner conducive to properly responding to actual phishing attacks. Neither employee responses to phishing engagements initiated on behalf of Management nor employee status as "recurring-clicker" shall (1) appear in employees electronic Official Personnel Files (OPF), or (2) be used for disciplinary purposes in any fashion. Neither individual employees nor any subset groups of employees shall be targeted in these anti-phishing emails, nor treated differently than other employees.

(5) Management shall send a yearly written notice to be distributed to GESTA and AFGE employees, which is to be provided to Labor for review for comments and edits at least five (5) business days in advance. This initiative will not start prior to 30 days from the signing of this MoA. The definition of a "recurring-clicker" shall also be included in the notification to employees.

(6) Employees are permitted to submit challenges to this required training and the training shall be held in abeyance until the complete grievance process, e.g., all Grievance STEPs, and any arbitration resulting thereof is also completed in accordance with employees' respective Collective Bargaining Agreement (CBA). If the required training is not upheld in the grievance/arbitration process then the employee shall not be required to take the training.

(7) The Center shall maintain records of the number of employees required to undergo the training, inclusive of bargaining (with names) and non-bargaining unit employees (without individual names), and their codes, as well as those employees who have completed the training. This information will be provided to Labor during the initial training at the end of this year and thereafter at least once every calendar year.

(8) The application of the subject policy shall be fair, equitable, and consistent with existing statutes, government-wide regulations, and collective bargaining agreements.

POINTS OF CONTACT

Sergio R. McKenzie
Chief Information Security Officer
Sergio.R.McKenzie@nasa.gov
(301)-286-0877

Anel Flores
Co-Chair, GSFC Labor Caucus
Anel.Flores-1@nasa.gov
301-286-7841

OTHER PROVISIONS

Nothing in this Agreement is intended to conflict with current law or regulation. If a clause of this Agreement is inconsistent with such authority, then that clause shall be invalid, but the remaining terms and conditions of this Agreement shall remain in full force and effect.

EFFECTIVE DATE

This MoA shall take effect immediately upon the signature of both parties.

MODIFICATION/PERIODIC REVIEW/RECONSIDERATION

Either Labor or Management has the right to request a review of this MoA at any time or as mutually agreed upon by all parties to terminate this agreement. Changes to this MoA may be made with notice and opportunity to bargain, as required by the applicable law.

FOR MANAGEMENT

Nancy A Abell 11/27/2017

Nancy A. Abell — Date
GSFC Associate Director

for Christina Lafountain 11/27/2017

Christina Lafountain — Date
GSFC Labor Relations Officer

FOR LABOR

Anel Flores 11-15-2017

Anel Flores — Date
President, IFPTE Local 29

BEN ROBBINS Digitally signed by BEN ROBBINS Date: 2017.11.16 15:40:42 -05'00'

Ben C. Robbins — Date
Vice-President, AFGE Local 1923