

POLICE DEPARTMENT

COUNTY OF MAUI



ALAN M. ARAKAWA
MAYOR
MM/lu
OUR REFERENCE
YOUR REFERENCE

55 MAHALANI STREET
WAILUKU, HAWAII 96793
(808) 244-6400
FAX (808) 244-6411

RECEIVED
2017 AUG 29 AM 9:47
OFFICE OF THE MAYOR

TIVOLI S. FAAUMU
CHIEF OF POLICE
DEAN M. RICKARD
DEPUTY CHIEF OF POLICE

August 28, 2017

OFFICE OF THE COUNTY CLERK
County of Maui

AUG 31 2017 4:33 am
dy

Honorable Alan M. Arakawa
Mayor, County of Maui
200 South High Street
Wailuku, Hawaii 96793

For transmittal to:

Honorable Mike White, Chair
and Members of the Maui County Council
200 South High Street
Wailuku, Hawaii 96793

APPROVED FOR TRANSMITTAL
Alan Arakawa 8/30/17
Mayor Date

Dear Chair White and Members:

SUBJECT: INTERGOVERNMENTAL AGREEMENT WITH THE UNITED STATES
SECRET SERVICE

Pursuant to County Code 2.20.020, we are hereby transmitting a bill for an ordinance authorizing the Mayor of the County of Maui to enter into an intergovernmental agreement with the United States Secret Service (USSS) regarding payment of expenses from Joint Operations between USSS and the Maui Police Department. This MOU establishes the procedures and responsibilities of both the Maui Police Department and USSS for the reimbursement of certain overtime costs and other expenses in relation to the USSS's Hawaii Electronic Crimes Task Force.

Thank you for your attention to this matter. If you have any questions, please feel free to contact our accountant, Lesley Ann Uemae, at ext. 6309.

Sincerely,

Tivoli S. Faaumua
TIVOLI S. FAAUMU
Chief of Police

COUNTY COMMUNICATION NO. 17-352

This information is being provided as additional information related to a proposal for the Maui Police Department to join and participate in the recently established HAWAII ELECTRONIC CRIMES TASK FORCE which is headed by the United States Secret Service's Honolulu Field Office.

The United States Secret Service (USSS) developed the Electronic Crimes Task Force (ECTF) to increase the resources and skills by which State, Local and Federal Law Enforcement agencies team with prosecutors, private industries and others to maximize what each has to offer in an effort to combat criminal activity. The common purpose is the prevention, detection, mitigation and investigation of attacks on the nation's financial and critical infrastructures. The first ECTF was formed in 1995 in New York. Since then, the USSS has established a nationwide network of ECTF's around the country which collectively provide necessary support and resources to field investigations that meet any one of the following criteria:

- Significant economic or community impact,
- Participation of organized criminal groups involving multiple districts or transnational organizations, and
- Use of schemes involving new technology.

Investigations conducted by ECTFs include such crimes as:

- Computer generated counterfeit currency,
- Bank Fraud,
- Virus and worm proliferation,
- Access device fraud,
- Telecommunications fraud,
- Internet threats,
- Computer system intrusions and cyber-attacks,
- Phishing/spoofing,
- Assistance with Internet-related child pornography and exploitation, and
- Identity Theft

In 2016, USSS personnel reached out to our department to offer specialized training in this field of expertise. Since then, we have been fortunate enough to have sent several of our detectives to various related courses through funding from the federal government and at no cost to our department. The detectives who have gone through these courses have related their very positive experiences regarding knowledge gained as well as expanding their investigative fields of view.

One of the drawbacks in addressing electronic crimes is the need for proper and sometimes expensive equipment that is needed to conduct these investigations. Without the proper equipment, training and know-how, electronic crimes can become an insurmountable problem due to the complexity and need for specialized equipment required to address these crimes.

After becoming more familiar with the USSS training opportunities, I was able to speak with USSS personnel who expressed the opportunity for our department and designated personnel to become a part of the USSS Hawaii Electronic Crimes Task Force. Once we had

personnel attend the training courses, our department became eligible to participate in the HECTF.

Benefits for participating in the HECTF, besides those already mentioned, would include funding for equipment, training and overtime when the instances arise. As of this date, MPD has sent one of our officers to attend specialized training where our department becomes eligible to receive the necessary equipment for that officer to become a forensic examiner.

As computer-related crimes have increased throughout the years, not only in the number of instances, but also in their complexity, we have seen the need arise for officers to receive specialized training in addressing these crimes. Hindrances for our county and department in the past have been the requirement of procuring specialized equipment which may be very expensive as well as keeping our officers up to date in the most current practices and methodologies to investigate these types of crimes.

If our police department is able to participate in the Hawaii Electronic Crimes Task Force, those barriers that we have experienced in the past may no longer be obstacles as training, equipment and funding for these types of crimes may be obtained through federal funding associated through the United States Secret Service and the Hawaii Electronic Crimes Task Force program.

A more detailed explanation of the HECTF has been provided by the USSS and is submitted as an attachment.

In order to participate in the HECTF, a Memorandum of Understanding (Exhibit 1) will have to be entered into by our county/police department and the United States Secret Service. This memorandum is attached for your reference.

Thank you for your time and consideration in this matter.

ORDINANCE NO. _____

BILL NO. _____ (2017)

A BILL FOR AN ORDINANCE AUTHORIZING THE MAYOR OF THE
COUNTY OF MAUI TO ENTER INTO AN INTERGOVERNMENTAL AGREEMENT
WITH THE UNITED STATES SECRET SERVICE (USSS)
REGARDING PAYMENT OF EXPENSES FROM JOINT OPERATIONS BETWEEN
USSS AND THE MAUI POLICE DEPARTMENT

BE IT ORDAINED BY THE PEOPLE OF THE COUNTY OF MAUI:


SECTION 1. Purpose. The County of Maui and the United States Secret Service (USSS) wish to enter into a Memorandum of Understanding (“the Agreement”) to establish the procedures and responsibilities of both the Maui Police Department and USSS for reimbursement of certain overtime costs and other expenses incurred during participation of the Maui Police Department in USSS’s Hawaii Electronic Crimes Task Force operations, as more fully described in the “Memorandum of Understanding Between the Maui Police Department and the United States Secret Service” attached hereto and incorporated herein by reference as Exhibit “1.”

Section 2.20.020, Maui County Code, provides that, unless authorized by ordinance, the Mayor shall not enter into any intergovernmental agreement or any amendment thereto which places a financial obligation upon the county or any department or agency thereof.

SECTION 2. Council authorization. Pursuant to Section 2.20.020, Maui County Code, the Council of the County of Maui hereby authorizes the Mayor to execute the Agreement, all other necessary documents relating to the Agreement, and any amendments thereto.

SECTION 3. Effective date. This ordinance shall take effect upon its approval.

APPROVED AS TO FORM
AND LEGALITY:



JERRIE L. SHEPPARD
Deputy Corporation Counsel
County of Maui
(LF 2017-0338)

**MEMORANDUM OF UNDERSTANDING SERVICE
BETWEEN THE MAUI POLICE DEPARTMENT
AND 2017 MAY 25 P 5:47
THE UNITED STATES SECRET SERVICE
HONOLULU, HAWAII**

The Maui Police Department and the United States Secret Service (USSS) enter into this memorandum of understanding (MOU), which becomes effective with the signatures of both parties and remains in effect until terminated by the mutual agreement of the Maui Police Department and the USSS or upon 30 day written notice by either party to this agreement.

I. AUTHORITY

This MOU is established pursuant to provisions of the Treasury Forfeiture Fund Act of 1992, 31 USC 9703, as amended. This act established the Department of the Treasury Forfeiture Fund and authorized the payment of certain overtime expenditures, travel, fuel, training, equipment and other similar costs of State and Local law enforcement officers, that are involved in joint operations, with a Department of the Treasury law enforcement organization, as prescribed in 31 USC 9703 (a)(1)(I)(hereinafter "overtime costs and other expenses").

II. PURPOSE

This MOU establishes the procedures and responsibilities of both the Maui Police Department and the USSS for the reimbursement of certain overtime costs and other expenses pursuant to 31 USC 9703.

III. CONDITIONS AND PROCEDURES

The parties agree to the following conditions:

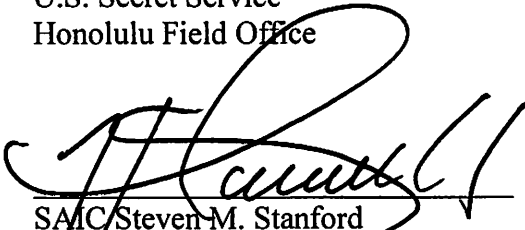
- a. The Maui Police Department may request reimbursement of payment of overtime costs and other expenses directly related to work performed by its officer(s) assigned to assist the U.S. Secret Service's Hawaii Electronic Crimes Task Force in conducting official investigations. The Maui Police Department will submit all requests for reimbursement payments, together with appropriate documentation, to the U.S. Secret Service's Task Force Supervisor. Request for reimbursement will be based solely upon overtime worked and other expenses performed on behalf of the U.S. Secret Service Hawaii Electronic Crimes Task Force.
- b. All reimbursement hours of overtime costs and all other expenses covered under this MOU must be approved and certified by the U.S. Secret Service Task Force supervisor. The reimbursable overtime payments will be based upon the actual hourly overtime rate, exclusive of matching employer contributions for any taxes or benefits.

- c. The U.S. Secret Service Task Force supervisor will forward all approved reimbursement requests through the Special Agent in Charge (SAIC) Asset Forfeiture Division, Office of Investigations, to the Treasury Forfeiture Fund's payment agent, U.S. Customs National Finance Center (NFC).
- d. During the period of assignment to the Hawaii Electronic Crimes Task Force, the Maui Police Department will remain responsible for establishing the salary and benefits, including overtime of the officer(s) assigned to the Task Force and making all payments due them. Reimbursement under this MOU is contingent upon the availability of mandatory funds allocated to the U.S. Secret Service through the Department of the Treasury Forfeiture fund.
- e. The Maui Police Department shall permit and have readily available for examination and auditing by the U.S. Secret Service, the Department of Treasury, the Comptroller of the United States, and any of their duly authorized agents and representatives, any and all records, documents, accounts, invoices, receipts or expenditures relating to this agreement. They shall maintain all such records and reports until all audits and examinations are completed and resolved, or for a period of three (3) years, whichever is sooner.
- f. Payments may be made to the extent they are included in the U.S. Secret Service Fiscal Year Plan and the monies are available within the Department of Treasury Forfeiture Fund to satisfy the request(s) for reimbursable expenses. It should also be understood that the total amount(s) made available to the U.S. Secret Service through the Department of the Treasury Forfeiture Fund, for reimbursement to the Maui Police Department, could change at any time.
- g. Pursuant to the Treasury Executive Office for Asset Forfeiture (TEOAF) directive number 18, the maximum reimbursement entitlement for overtime costs to any one law enforcement official cannot exceed fifteen-thousand (\$15,000.00) dollars during the fiscal year.
- h. This document does not obligate funds. Funding authority will be provided through other documents.
- i. The Maui Police Department shall provide the U.S. Secret Service within 10 days of the signing of this MOU, with their agency's mailing address, contact name, telephone number and tax identification number. Further, this agency must provide the name, account number and ABA routing number of the financial institution where the (Name of Law Enforcement Agency) wants the Electronic Funds transfer (EFT) payment deposited for the reimbursement of overtime salary costs. Failure to provide this information within the prescribed period of time will nullify this MOU agreement.

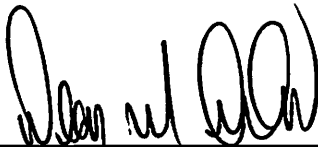
IV. REVISIONS

The terms of this MOU may be amended upon the written approval of both the Maui Police Department and the U.S. Secret Service. Such amendment is effective upon the date of approval.

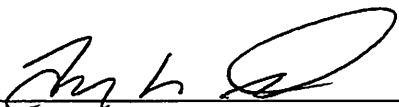
U.S. Secret Service
Honolulu Field Office


SAIC Steven M. Stanford
Date: 6/8/2017

Maui Police Department


Chief Tivoli Faamu
Date: 5/19/17

U.S. Secret Service, Office of Investigation
Criminal Investigative Division

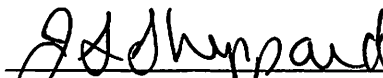

SAIC - Criminal Investigative Division
Date: 7/5/17

County of Maui Mayor

Mayor Alan Arakawa

Date: _____

APPROVED AS TO FORM
AND LEGALITY:


JERRIE L. SHEPPARD
Deputy Corporation Counsel
County of Maui
2017-0338

The United States Secret Service (USSS) recognizes partnering as an integral part of its success in the performance of both its protective and investigative missions. Whether it is securing a venue for the President of the United States or investigating a complex financial crime scheme, the USSS relies on its relationships and actively looks to work together with their local counterparts to get the job done.

The USSS was created in 1865 as a part of the U.S. Treasury Department to investigate the counterfeiting of U.S. currency, which was the most prevalent financial crime of that era. In modern times, almost all financial crime involves the use of computer technology. In order to combat this emerging threat, the USSS looked again to leverage its partnerships in the 1990s and created the first Electronic Crime Task Forces (ECTFs) in major cities across the United States.

Today, as cyber criminals have become more prolific by operating in environments such as the dark web and as we see instances of network intrusion, malicious software and unauthorized use of personal identification information on the rise, the need to work together and leverage relationships has never been more evident.

The Hawaii Electronic Crimes Task Force (HECTF) became operational within the last year and is positioning itself to mitigate, disrupt, deter and investigate the activities listed above which are sadly not uncommon in Hawaii and the Pacific Region and have significant community impact.

The law enforcement portion of the HECTF includes representatives of Federal, State and local law enforcement departments and agencies. Within the last year, the USSS Honolulu Field Office's HECTF has entered into Memorandums of Understanding (MOUs) with the Honolulu Police Department, Hawaii Police Department and the Hawaii Department of the Attorney General- Investigations Division.

As HECTF members can attest, the benefits of formal membership extend beyond force multiplication in the investigation of complex cyber related crimes. The HECTF provides training opportunities to its local law enforcement partners at the National Computer Forensics Institute that are fully funded by the USSS. Another benefit of formal membership is the availability of the HECTF's Federal funding through the U.S. Treasury Department's Treasury Executive Office for Asset Forfeiture (TEOAF). These TEOAF funds are available for the reimbursement of approved expenditures that include law enforcement overtime for task force investigations, equipment, investigative travel, as well as individual training courses that support the HECTF's mission.

A more detailed description of USSS ECTFs is provided below:

United States Secret Service Electronic Crimes Task Force Doctrine

Mission:

The United States Secret Service Electronic Crimes Task Forces are a strategic alliance of law enforcement, academia and the corporate sector, dedicated to investigating, disrupting, and

detering homeland security related cybercrime, as well as cyber-related high consequence events related to Secret Service missions and critical infrastructure sectors.

Overview:

On October 26, 2001, President Bush signed into law H.R. 3162, the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot) Act of 2001.” In drafting this particular legislation, Congress recognized the Secret Service philosophy that our success resides in the ability to bring academia, law enforcement and private industry together to combat crime in the information age. As a result, the U.S. Secret Service was mandated by this Act to establish a nationwide network of Electronic Crimes Task Forces.

The United States Secret Service’s Electronic Crimes Task Forces seek to prioritize investigative cases that involve electronic crime. The ECTFs are directed to concentrate their resources in the following three areas:

1. **Cyber-Protection:** secure environmental elements that touch Secret Service missions, state and local government leaders, and critical infrastructure sectors that are controlled by computer systems and have access to the Internet through the Critical System Protection Program.
2. **Cyber-Investigation:** target, pursue, and arrest individuals and groups that engage in cyber-criminal activity that has significant economic or community impact; involvement of organized criminal groups involving multiple districts or transnational organizations; or the utilization of schemes involving new technology.
3. **Cyber Tools:** develop cyber-based tactics, technologies, methodologies, and training to facilitate operational and business processes throughout the Secret Service, and build a workforce that effectively combats technology-based threats through the Electronic Crimes Special Agent Program.

Cyber – Protection

Members of an ECTF should work with public and private corporations identified as part of the United States critical infrastructure, to conduct CSP advances on the facilities in their districts. These advances should concentrate on assessing and mitigating the risk of disruption or destruction of information systems that affect the safety of persons protected by the Secret Service.

Cyber - Investigative Priorities

- **Core violations**
 - The ECTFs are responsible for investigating crimes which are considered core violations for The United States Secret Service.

- The investigation of core violations will also benefit the law enforcement community and private industry at large by providing a strong base of knowledge and expertise in investigating complex and technologically intensive cases.
- **High Dollar Loss**
 - The investigation of high dollar loss cases is a priority for the ECTFs.
 - High dollar loss cases are usually multi-jurisdictional and difficult for State and Local agencies to successfully prosecute.
 - Additionally, through the application of federal asset forfeiture laws, it is possible to recoup some of the financial loss and reinvest it back into the community.
- **Large Impact to the Community**
 - The ECTFs investigate cases which have a large impact on the community.
 - Cases, such as identity theft, credit card fraud, electronic debit card fraud, cellular telephone fraud and many other technologically advanced cases are investigated by the ECTFs.
- **Trans-national or multi-district investigations**
 - The ECTFs are able to help State and Local agencies across State and National boundaries through international liaison programs and foreign offices.
 - Partnerships in the ECTFs allow for the utilization of Federal resources in order to successfully solve and bring to prosecution cases which may have been outside of the scope of some smaller jurisdictions.
 - Provide strategies to Field Offices through cyber intelligence collection and analysis conducted by headquarters.
- **Investigation involves new technology or scheme**
 - Participation in the ECTFs allows for access to training and hands on experience for State and Local agencies which may have budgetary constraints.
 - ECTFs act as a knowledge base, joining the education and expertise of federal, state/local law enforcement along with corporate and academia sectors to successfully investigate increasingly complex and technologically based cases.

Cyber – Tools

Members of the ECTF should work with corporations and academia to develop and deliver innovative classes and curricula that address changing priorities and trends affecting the ability to successfully secure information systems.

Electronic Crimes Task Force Structure

The Secret Service has developed a standardized cadre of specialized trained agents and local law enforcement officers to work as members of its Electronic Crimes Task Forces. Each task force should have members trained in the following:

- Computer Forensics (CP)

- Network Intrusions (NITRO)
- Critical Systems Protection (CSP)
- Mobile Wireless Analysis