

## RESOLUTION CITY OF SAINT PAUL, MINNESOTA

Presented by \_\_\_\_\_

1 WHEREAS, the City of Saint Paul, Police Department is requesting authorization to enter into two (2) agreements  
 2 with the Federal Bureau of Information (FBI) which are the Joint Powers Agreement to participate in the Minnesota  
 3 Cyber Crime Task Force (MCCTF) and the Memorandum of Agreement reimbursing for expenditures and  
 4 equipment purchased for the MCCTF, and  
 5

6 WHEREAS, the mission of the MCCTF is to investigate and apprehend high technology criminals and to protect our  
 7 communities by preventing high technology crime and national security threats involving computers and computer  
 8 networks, and  
 9

10 WHEREAS, a 2011 financing and spending plan needs to be established for these funds; and  
 11

12 WHEREAS, the Mayor pursuant to Section 10.07.1 of the Charter of the City of Saint Paul, does certify that there  
 13 are available for appropriation funds of \$5,000 in excess of those estimated in the 2011 budget; and  
 14

15 WHEREAS, the Mayor recommends that the following addition be made to the 2011 budget:

16	<b>001 Police - General Fund - Activity (04229-SIU)</b>			
17	<b>Account(Object Code)</b>		<b>CURRENT BUDGET</b>	<b>CHANGES</b>
18			<b>AMENDED BUDGET</b>	
19	<b>Spending Changes</b>			
20	0370	Computer		5,000
21				5,000
22			<b>TOTAL:</b>	<b>0</b>
23	<b>Financing Changes</b>			
24	4398	Services - Special Projects		5,000
25				5,000
			<b>TOTAL:</b>	<b>0</b>

26 THEREFORE BE IT RESOLVED, that council authorized the City of Saint Paul to enter into and Chief Thomas  
 27 Smith to implement the attached agreements, and  
 28

29 THEREFORE BE IT RESOLVED, that the Saint Paul City Council approves these changes to the 2011 budget.

	Yeas	Nays	Absent
Bostrom			
Carter			
Harris			
Helgen			
Lantry			
Stark			
Thune			

Requested by Department of: **POLICE**

By: \_\_\_\_\_  
 Approved by the Office of Financial Services

By: \_\_\_\_\_  
 Approved by City Attorney

By: \_\_\_\_\_  
 Approved by Mayor for Submission to Council

By: \_\_\_\_\_

Adopted by Council: Date \_\_\_\_\_

Adoption Certified by Council Secretary

By: \_\_\_\_\_

Approved by Mayor: Date \_\_\_\_\_

By: \_\_\_\_\_

**MEMORANDUM OF AGREEMENT**

**BETWEEN**

**THE FEDERAL BUREAU INVESTIGATION**

**AND**

**ST. PAUL POLICE DEPARTMENT**

**1. PURPOSE:** The purpose of this Memorandum of Agreement (MOA) between the Federal Bureau of Investigation (FBI) and the City of St. Paul Police Department, hereinafter referred to as the "parties", is to define the scope of work and responsibilities of the parties concerning reimbursement for the equipment costs associated with their participation in the FBI's Minnesota Cyber Crime Task Force.

**2. BACKGROUND:** The MCCTF is jointly sponsored by the FBI and the United States Secret Service and began in January 2006. The St. Paul Police Department (SPPD) has been a charter member of the MCCTF and also works closely with a the Internet Crimes Against Children (ICAC) Task Force for Minnesota as well as a number of local departments in combating the sexual exploitation of children. SPPD also provides forensic examination and digital evidence recovery and review services for a host of investigators, and has identified and evaluated equipment and software applications that are required to expand evidence review capabilities in Minnesota.

**3. AUTHORITY:** The FBI is entering into this MOA under the authority provided by 28 U.S.C. § 533 and 28 C.F.R. § 0.85.

**4. SCOPE:** This MOA defines the terms and conditions for reimbursement by the FBI of expenditures incurred by St. Paul Police Department in equipping the task force with the following:

- Contingent on the availability of funds through the FBI's Cyber Division, Cyber Criminal Unit 3, the FBI will seek funding for St. Paul Police Department reimbursement for equipment for the Minnesota Cyber Crime Task Force.
- The following are expenditures, submitted through invoices from St. Paul Police Department to the FBI for the equipment provided for use by the Minnesota Cyber Crime Task Force:

VENDOR : ITEM DESCRIPTION	QUANTITY REQUESTED	QUANTITY APPROVED	UNIT PRICE	TOTAL
Intelligent Computer Solutions: IM Solo-4 Forensic Hard Drive Acquisition / Uploader	1	1	\$ 3,099	\$ 3,099

VOOM Technologies, Inc. Shadow 2 Computer Forensic Analysis Device	1	1	\$ 1,615	1,615
Total				\$ 4,714

**5. FUNDING:** The FBI hereby agrees to spend a sum of money not to exceed \$5,000 for reimbursement to St. Paul Police Department for the aforementioned equipment provided for use by the Minnesota Cyber Crimes Task Force.

**6. LIABILITY:** The parties agree that each party is responsible for the negligent and wrongful acts and omissions by its employees. In addition, the parties agree that should a claim arise under the terms and conditions of the Federal Tort Claims Act (FTCA), Title 28, United States Code, Sections 1346 and 2671 et seq., for the negligent and wrongful act and omission by either parties' employee in the performance of assigned task force duties, the FBI shall be responsible for the investigation and disposition of said claim. Nothing herein should be construed as supplanting any applicable statute, rule or regulation.

**7. POINTS OF CONTACT:** The FBI and the St. Paul Police Department will assign points of contact (POCs) for this agreement. The POCs will address and resolve all issues related to this agreement. The parties agree to coordinate liability issues, jurisdictional matters, and any other issues through their designated POC.

**8. SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOA will be resolved only by consultation between the parties and will not be referred to a local, state, or federal court.

**9. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION**

a. All activities of the parties under this MOA will be carried out in accordance with the terms and conditions of this MOA.

b. Except as otherwise provided, this MOA may be amended by the mutual written consent of the parties' authorized representatives.

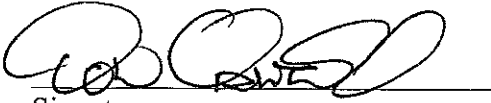
**10. FORCE AND EFFECT**

This MOA, which consists of 10 Sections on 3 pages, will enter into effect upon signature of all parties and will remain in effect for the duration of the Minnesota Cyber Crime Task Force.

This MOA is the complete and exclusive statement of agreement between the parties with respect to the FBI's reimbursement to St. Paul Police Department for the costs associated with the purchase of the above listed equipment to be utilized by the Minnesota Cyber Crime Task Force. This MOA supercedes all written and oral proposals and other communications between the parties. All activities of the parties under this MOA will be carried

out in accordance with the terms and conditions of this MOA. Nothing in this MOA is intended to create, nor does it create, an enforceable legal right or private right of action. The foregoing represents the understandings reached between the FBI and St. Paul Police Department upon the matters referred to herein.

**FOR THE FEDERAL BUREAU OF INVESTIGATION**



Signature  
Donald E. Oswald  
Special Agent in Charge

8/29/11  
Date

\_\_\_\_\_  
Signature  
FBI Contracting Officer

\_\_\_\_\_  
Date

**FOR THE ST. PAUL POLICE DEPARTMENT**

\_\_\_\_\_  
Signature  
Thomas E. Smith  
Chief  
St. Paul Police Department

\_\_\_\_\_  
Date

# MINNESOTA CYBER CRIME TASK FORCE MEMORANDUM OF UNDERSTANDING

- A. **PARTIES.** This Memorandum of Understanding (MOU) is entered into by the following "Participating Agencies":
1. **Federal Bureau of Investigation (FBI)**  
(authorized pursuant to 28 USC 533, 534; 28 C.F.R. § 0.85)
  2. **St. Paul Police Department**
- B. **PURPOSE.** This MOU delineates the responsibilities and commitments of the Participating Agencies in the **Minnesota Cyber Crime Task Force (MCCTF)**. The MOU also outlines the mission and procedures for the CCTF, which are described in greater detail in the Standard Operating Procedures (SOP) utilized by the CCTF.
- C. **MISSION.** The mission of the MCCTF is to investigate and apprehend high technology criminals and to protect our communities by preventing high technology crime and national security threats involving computers and computer networks. The MCCTF is established on the premise that the capabilities of law enforcement agencies to investigate computer and high technology related crimes are enhanced in a task force setting involving the sharing of resources and expertise. The MCCTF will utilize its specialized resources to investigate, and to prevent when possible, criminal cases and national security threats when: (1) Computers and high technologies are the target of a crime; (2) Computers and high technologies are the principal instrumentality of a crime; or, (3) Computers and high technologies are misused to facilitate violations of other criminal laws or threats to the national security and a specialized understanding of technology is required for investigation or prosecution.
- D. **INVESTIGATIVE EXCLUSIVITY.** Matters designated to be handled by the MCCTF will not knowingly be subject to separate and/or independent outside law enforcement efforts by any of the participating or referring agencies. Each Participating Agency shall make proper internal notification regarding the MCCTF's existence and areas of investigation.
- E. **PROSECUTIONS.** A determination will be made for each MCCTF investigation on whether the matter should be submitted for filing in federal or state court. This determination shall be based on the evidence obtained and a consideration of which method of prosecution will result in the greatest benefit to the overall objectives of the MCCTF and the community.
- F. **DOCUMENTS AND AUTHORITIES INCORPORATED BY REFERENCE.** The Participating Agencies agree to abide by the separate document titled "Cyber Crime Task Force Standard Operating Procedures." The CCTF SOP, as updated from time to time, is fully incorporated by reference into this MOU.
- G. **ADMINISTRATIVE RESPONSIBILITIES**
1. Shared Responsibilities: All participants of the MCCTF acknowledge that this is a joint operation with all Participating Agencies acting for a common goal. Accordingly, the mission and objectives of the MCCTF will be a shared responsibility of the Participating Agencies.
  2. Lead Agency: The FBI is the lead agency for the MCCTF and agrees to overall management responsibilities for the task force, including but not limited to record keeping and daily responsibility for personnel work assignments and investigative matters.

Official Law Enforcement Use Only

Standard Cyber Crime Task Force MOU (March 2006)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

3. FBI Program Manager: The daily operational control, management, supervision of, and responsibility for operations of the MCCTF shall be vested in an FBI Program Manager. The FBI Program Manager shall be a sworn law enforcement officer (an FBI Special Agent or Supervisory Special Agent) assigned by his/her respective FBI Field Office to the MCCTF. The term of office of the FBI Program Manager generally shall be a minimum of one (1) year, full-time, to commence upon appointment.
4. Participating Agency Team Leader: Day-to-day operational matters may be assigned by the FBI Program Manager to a Team Manager. The Team Manager shall be from a Participating Agency other than the FBI and shall be selected by the FBI in consultation with all MCCTF Participating Agencies. The Team Manager shall be a full-time employee assigned to the MCCTF. The term of office of the Team Manager generally shall be a minimum of one (1) year, full-time, to commence upon appointment.

## H. PERSONNEL

1. Membership: The MCCTF shall consist of a combined body of investigators and support personnel from the Participating Agencies.
2. No Employment by the MCCTF: The MCCTF does not directly or indirectly employ any personnel assigned to it. The MCCTF is established for the coordination of applicable investigations and does not establish employer-employee relationships with the personnel assigned to the MCCTF from the Participating Agencies.
3. Responsibility for Conduct: Personnel assigned to the MCCTF may not engage in any activity which, either in appearance or in fact, conflicts with their duties at the MCCTF or reasonably impeaches the independence of their work for the MCCTF. In addition to the requirements set forth in this MOU and the accompanying SOP, each Participating Agency shall ensure that their employee participants remain subject to and adhere to the standards of conduct, personnel rules, regulations, laws, and policies applicable to those of their respective agency.
4. Assignment to the MCCTF: Personnel selections for the MCCTF are at the discretion of the FBI and each respective Participating Agency. Personnel will be selected based on the needs of the MCCTF and the Participating Agencies. As a general matter, all personnel shall work in a full-time capacity at the MCCTF (and at a minimum not less than 3 days a week) and make a minimum two-year work commitment to the MCCTF due to the specialized nature of the work and applicable training.

## I. INFORMATION MANAGEMENT

1. Records and Reports: All MCCTF investigative records will be maintained at the MCCTF location or the local FBI Field Office. Investigative documents will be stored on the FBI's electronic databases in order to enhance national information sharing among task forces and other investigators. Classified information shall not be placed in a non-Federal Participating Agency's files or maintained outside of an accredited MCCTF location unless approved in advance and in writing by an FBI Security Officer.
2. Non-Disclosure Agreement. MCCTF information only may be disseminated on a need-to-know basis and as expressly permitted. No MCCTF information may be disseminated outside of the MCCTF without the express permission of the FBI and in accordance with the applicable laws and internal regulations, procedures, or agreements between the FBI and other agencies that would permit such agencies, including MCCTF participants' employing agencies, to receive FBI information directly.
3. Media: No member of the MCCTF will unilaterally discuss or otherwise reveal information relating to MCCTF investigations, or other FBI related investigations known to them, to any media representatives. All releases of information to the media on MCCTF matters will be mutually agreed upon and coordinated jointly under the supervision of the FBI Program Manager or Team Manager.

J. **LIABILITY.** The FBI makes no representation that the United States will provide legal representation or indemnification to any law enforcement officer or employee assigned to the MCCTF. Legal representation and indemnification by the United States is determined by the Department of Justice (DOJ) on a case-by-case basis pursuant to legal standards and DOJ policy.

K. **SALARIES AND FUNDING**

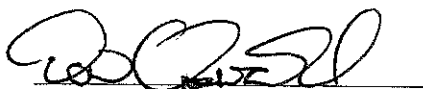
1. Salary and Compensation: Salaries, benefits, taxes, and withholdings of MCCTF members will be paid by their respective agencies.
2. Overtime: Overtime may be compensated to MCCTF members by their respective agencies in accordance with their applicable overtime provisions or by the FBI in accordance with a separate Cost Reimbursement Agreement.
3. Funding: This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds; this MOU is instead a basic statement of the understanding between the parties of the tasks and methods required for a successful MCCTF. Unless otherwise agreed in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

L. **DURATION AND MODIFICATION OF THE MOU.** The term of this MOU shall be for the duration of the MCCTF's operations, contingent upon approval of necessary funding, but may be terminated at any time upon the written mutual consent of the agencies involved. A Participating Agency retains the right to terminate its participation by giving 30 days written notice of its intent to terminate. Should a Participating Agency terminate its participation, it must return any equipment to the supplying entity. Similarly, as soon as practicable consistent with ongoing investigations, remaining agencies will return to a withdrawing agency any unexpended equipment the withdrawing agency may have supplied during its MCCTF participation. Any modification of this MOU will be effected with the written mutual consent of the involved parties. This MOU may be signed in counterparts.

M. **NO THIRD PARTY RIGHTS.** This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party (other than a Participating Agency of this MCCTF entering into a similar MOU with the FBI) against the parties hereto, the United States, or the officers, employees, agents, or other associated personnel thereof.

N. **EFFECTIVE DATE AND ADDITIONAL PARTIES.** As among the original parties, this MOU shall become effective when signed and dated by the FBI and the duly authorized representative of at least one other agency. The parties anticipate that the FBI will enter into similar MOUs with other Participating Agencies.

SO AGREED on behalf of the entities/organizations below:

  
Name: Donald E. Oswald  
Title: Special Agent in Charge  
FBI-Minneapolis

\_\_\_\_\_  
Name:  
Title: Contracting Officer  
FBI

\_\_\_\_\_  
Name: Thomas E. Smith  
Title: Chief  
St. Paul Police Department

Official Law Enforcement Use Only

Standard Cyber Crime Task Force MOU (March 2006)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

CYBER CRIME TASK FORCE  
(CCTF)

STANDARD OPERATING PROCEDURES  
(SOP)

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*



## A MESSAGE FROM THE FBI

The first FBI-led Cyber Crime Task Force (CCTF) was established in Pittsburgh in 1997. Since that time, the need has grown even stronger for pulling the law enforcement community together to meet the challenges of high technology crime. The task force model has proven successful to combat a wide range of the most challenging threats to our nation, including domestic and international terrorism, narcotics smuggling, organized crime and, now, cyber exploitation.

Many members of the CCTF have also been members of other task forces, and their prior experience and insights will prove invaluable to this effort. Others will find their service with the CCTF to be an entirely new undertaking; we look forward to their fresh ideas and we welcome them to our expanding integrated law enforcement network.

Working together, pooling our unique capabilities, resources, and energy, we are confident that the greater law enforcement community can and will make considerable progress in preventing cyber crime, protecting our critical infrastructures, and bringing to justice those who would take advantage of ever-changing technologies to do us harm. We wish you every success.

**Official Law Enforcement Use Only**

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

## TABLE OF CONTENTS

I.	CCTF PRIORITIES AND CASE ASSIGNMENTS .....	-1-
	Investigative Priorities. ....	-1-
	Non-investigative Priorities. ....	-1-
II.	ORGANIZATIONAL STRUCTURE .....	-1-
	Law Enforcement/Intergovernmental Entity. ....	-1-
	Daily Operational Control: FBI Program Manager and Participating Agency Team Manager. ....	-2-
III.	ASSIGNMENT OF CASES/EXCLUSIVITY OF DUTIES DURING ASSIGNMENT TO THE CCTF ..	-3-
IV.	OPERATIONAL MATTERS .....	-3-
	Attorney General Guidelines. ....	-3-
	Field Tactical Operations. ....	-3-
	Undercover Operations. ....	-4-
	Officer Involved Incidents. ....	-5-
V.	INVESTIGATIVE AND EVIDENTIARY PROCEDURES .....	-5-
	No Superseding Standard of Care, Duty or Conduct. ....	-5-
	Applicable Investigative Legal Process. ....	-5-
	Report Format. ....	-5-
	FBI Databases and Information Systems. ....	-5-
	Forensic Examination Procedures. ....	-6-
VI.	ADMINISTRATIVE PROCEDURES .....	-7-
	Cross-deputation of Sworn Personnel .....	-7-
	Intergovernmental Personnel Act Assignments to Federal Agencies .....	-8-
	Personnel Administrative Issues .....	-9-
	Personnel Financial Issues .....	-10-
VII.	NON-DISCLOSURE OF INFORMATION/MEDIA POLICY .....	-13-
	Non-Disclosure Agreement. ....	-13-
	Media Inquiries Referred to the FBI Program Manager or the Team Manager. ....	-13-
VIII.	FINANCIAL AND CIVIL LIABILITIES IN GENERAL .....	-14-
	Federally Deputized Personnel. ....	-14-
	Federal Tort Claims Act. ....	-14-
	"Employee" of the United States. ....	-14-
	Scope of Employment. ....	-14-
	Petition for Scope of Employment Designation. ....	-14-
	Liability. ....	-14-
	Bivens Actions. ....	-15-

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

	Indemnification. ....	<u>-15-</u>
	Qualified Immunity. ....	<u>-15-</u>
	Representation. ....	<u>-15-</u>
	Notification of Claims. ....	<u>-15-</u>
<b>IX.</b>	<b>VEHICLES, EQUIPMENT, PROPERTY, AND GIFTS</b> .....	<u>-16-</u>
	Vehicles. ....	<u>-16-</u>
	Property of Participating Agencies Terminating Their Relationship with the CCTF. ....	<u>-16-</u>
	Certain Tangible Properties & Monies Acquired for CCTF Use. ....	<u>-16-</u>
	Intellectual Property. ....	<u>-17-</u>
	Educational Texts & Journals of Assignees. ....	<u>-17-</u>
	Assumption of Risk of Loss of Agency Property. ....	<u>-17-</u>
	Operational Supplies/Equipment. ....	<u>-17-</u>
	Gifts by Non-Governmental, Non-Participating Entities .....	<u>-18-</u>
<b>X.</b>	<b>COSTS</b> .....	<u>-18-</u>
<b>XI.</b>	<b>NO THIRD PARTY RIGHTS</b> .....	<u>-18-</u>
<b>XII.</b>	<b>MODIFICATIONS AND AMENDMENTS</b> .....	<u>-18-</u>
<b>XIII.</b>	<b>LEGAL CONSTRUCTION AND SEVERABILITY</b> .....	<u>-19-</u>

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

## I. CCTF PRIORITIES AND CASE ASSIGNMENTS

- A. Investigative Priorities. The investigative priorities of the CCTF shall be to prevent, detect, deter, and bring to justice, those persons and organizations involved in the following illegal activities:
1. The commission, attempted commission or conspiracy to commit any act which results in the compromise of the integrity, availability, or confidentiality of the contents of any computer, computer network, or similar devices using high technologies which results directly or indirectly in:
    - a. Physical injury to any person,
    - b. A threat to public health or safety, or
    - c. A threat to the National Security of the United States;
  2. The unlawful access, destruction of, or unauthorized entry into private or government computers or computer networks;
  3. The dissemination of software, often known as viruses and worms, that results in the criminal misuse of computers or computer networks;
  4. Identity theft facilitated by computers and high technology;
  5. Internet fraud;
  6. Software piracy and other unlawful uses of intellectual property;
  7. Internet threats; and,
  8. Sexual exploitation of children over the Internet, including child pornography.
- B. Non-investigative Priorities. The non-investigative priorities of the CCTF shall be as follows:
1. To facilitate and promote the sharing of federal and state law enforcement expertise and information about the investigation and prosecution of computer-related and technology-facilitated crime with law enforcement personnel and prosecutors; and
  2. To provide training and education for federal, state, and local law enforcement personnel and prosecutors regarding the investigation and prosecution of computer-related or technologically-facilitated crime.

## II. ORGANIZATIONAL STRUCTURE

- A. Law Enforcement/Intergovernmental Entity. The CCTF is a multi-jurisdictional task force comprised of personnel assigned primarily from law enforcement and criminal justice agencies. The CCTF is not intended to, and shall not, be deemed to have any independent legal status separate and apart from the individual sovereign governments from which its members emanate. Nothing contained in this SOP, or any accompanying MOU, shall be deemed or construed to create a partnership or joint venture, to create relationships of an employer-employee or principal-agent, or to otherwise create any liability for one agency whatsoever with respect to the indebtedness, liabilities, and obligations of the other agencies or any other parties.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

B. Daily Operational Control: FBI Program Manager and Participating Agency Team Manager.

1. The daily operational control, management, supervision of, and responsibility for operations of the CCTF shall be vested in an FBI Program Manager. **The FBI Program Manager shall be a sworn law enforcement officer (an FBI Special Agent or Supervisory Special Agent) assigned by his/her respective FBI Field Office to the CCTF.** The term of office of the FBI Program Manager generally shall be a minimum of one (1) year, full-time, to commence upon appointment.
2. Day-to-day operational matters may be assigned by the FBI Program Manager to a Team Manager. **The Team Manager shall be from a Participating Agency other than the FBI and shall be selected by the FBI in consultation with all CCTF Participating Agencies.** The Team Manager shall be a full-time employee assigned to the CCTF. The term of office of the Team Manager generally shall be a minimum of one (1) year, full-time, to commence upon appointment.
3. **FBI Program Manager and Team Manager Duties.** The FBI Program Manager shall be responsible for the day-to-day operations of the CCTF. Specifically, the FBI Program Manager, who may delegate as appropriate to the Team Manager, shall be responsible for proposing, implementing and enforcing such policies, procedures, practices and/or rules (in consultation with the Participating Agencies) as may be necessary or reasonably calculated to effectuate the purposes and mission of the CCTF, including:
  - a. assigning cases which are submitted to the CCTF;
  - b. prioritizing the assignment of cases in conformity with this SOP;
  - c. assigning responsibilities relating to administrative and/or educational duties;
  - d. establishing minimum qualification standards for prospective personnel offered for detail to the CCTF;
  - e. establishing additional ethical and conflict of interest guidelines for assignees and operations of the CCTF to supplement and augment the ethical and conflict of interest guidelines or rules established by each Participating Agency with respect to their individual assignees;
  - f. establishing standard forms and reports for use by the CCTF;
  - g. collecting, recording and submitting quarterly reports to the Participating Agencies regarding non-case specific data reflecting the operations and activities of the CCTF;
  - h. coordinating and controlling contacts with and responding to inquiries from members of the mass media in consultation with the appropriate Participating Agencies, or submitting law enforcement agency, if the inquiry is case specific;
  - i. requesting, when necessary, property, equipment, supplies or material from Participating Agencies;
  - j. maintaining an annual inventory of all property used, held by or on behalf of the CCTF, which inventory is to be recorded annually; and,
  - k. performing such other functions and duties as are reasonably related to the successful operation of the CCTF.
4. **Team Manager Renewal/Termination/Removal.** The term of office of the Team Manager may be renewed without limit by the FBI Program Manager, contingent upon the continued consent of the Team Manager's employing Participating Agency. Barring

extraordinary circumstances, the Participating Agency employing the Team Manager shall not withdraw consent except upon prior written notice of not less than thirty (30) days to the FBI Program Manager. The Team Manager shall serve until the earlier of: A) expiration of the term; B) his or her resignation; C) removal from the Team Manager position by the FBI Program Manager; or, D) removal from employment or the Team Manager position by his or her Participating Agency.

### III. ASSIGNMENT OF CASES/EXCLUSIVITY OF DUTIES DURING ASSIGNMENT TO THE CCTF

- A. Cases generally will be assigned for investigation to CCTF assignees at the discretion of the FBI Program Manager or the Team Manager without regard to the identity of the assignee's employing agency or the identity of the submitting agency, except that cases or categories of cases requiring specific security clearance or lawful authority (e.g., state or federal grand jury investigations requiring express court-authorized disclosure, Foreign Intelligence Surveillance Act (FISA) or other national security matters) may be specifically assigned by the FBI Program Manager based upon such criteria as he or she deems necessary.
- B. Cases generally will be assigned for investigation at the discretion of the FBI Program Manager or the Team Manager on the basis of case priority, as set forth above, and the experience and workload of an assignee. Except as authorized by the FBI Program Manager or the Team Manager, Participating Agencies agree that they shall not task their full-time CCTF assignees with other investigative or administrative obligations outside of those of the CCTF during the period of their assignment or permit them to take on such obligations.
- C. All assignees understand and agree that assignment to the CCTF does not create any right to investigate any specific matter or class of matters falling within the purview of the CCTF.

### IV. OPERATIONAL MATTERS

- A. Attorney General Guidelines. All federal agency participants and all federally deputized personnel will be subject to Attorney General Guidelines when acting on CCTF operational matters. All CCTF matters must be conducted pursuant to Attorney General Guidelines except for CCTF investigations that are exclusively being pursued as a state/local matter in which state/local prosecution is anticipated, federal prosecution is considered unlikely, and a state/local law enforcement officer is the primary investigative officer for the case.
- B. Field Tactical Operations. A field tactical operation is an investigative or enforcement action which is intended to interact with criminal suspects or witnesses and presents a greater than normal danger to agents, officers, and the public. Field tactical operations include planned searches of physical locations, coordinated surveillance, controlled buys, and controlled deliveries. Most undercover investigations will include one or more field tactical operations.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

Subject to the limited exception noted in subparagraph A above, all field tactical operations will be conducted pursuant to the **Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations**.

All field tactical operations will be documented with Tactical Operations Plan, describing at least the nature of the investigation, the intended procedures, the targeted individuals and locations, the personnel assignments for the duration of the operation, and emergency procedures.

- C. Undercover Operations. An undercover operation is an investigative or enforcement action where a law enforcement agent or officer interacts with criminal subjects and the agent/officer is not readily identified as a law enforcement officer. Undercover field tactical operations present a greater than normal danger to law enforcement officers/agents and the public.
1. Subject to the limited exception noted in subparagraph A above, all undercover operations will comply with the **U.S. Attorney General's Guidelines on FBI Undercover Operations**.
  2. All undercover field tactical operations will be documented with a Tactical Operations Plan.
  3. The undercover Tactical Operations Plan will address issues of officer and public safety as follows:
    - a. Whether the undercover officer will have case agent responsibilities during an undercover operation.
    - b. Whether the undercover officer will be armed during an undercover operation.
    - c. Whether the undercover officer will normally wear an electronic monitoring device or whether the plan specifically justifies not using such equipment.
    - d. Whether a security team shall be dedicated to the undercover officer's safety.
    - e. Whether other teams may be included to address perimeter security, communications, and surveillance as needed.
- D. Use of Confidential Informants. Any CCTF use or development of a confidential informant ("CI") will be in compliance with the **U.S. Attorney General's Guidelines Regarding the Use of Confidential Informants** including, but not limited to, for purposes of determining the suitability of a CI, the registration and use of a CI, payments to a CI, authorization for a CI to commit otherwise illegal activity, sharing sensitive investigative information with a CI, and protecting the identity of a CI.
- E. International Criminal Investigations. No matter being handled by the CCTF shall knowingly involve any international investigative activity (to include international communications) without FBI participation and approval. The FBI shall be responsible for coordinating, pursuant to Attorney General Guidelines, any extraterritorial criminal investigations.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

F. Officer Involved Incidents.

1. Any incident involving injury to CCTF personnel or damage to equipment will be reported to the Project Manager or Team Supervisor. The incident will also be reported to the Participating Agency according to its agency policy.
2. Any incident involving the discharge of a firearm by CCTF personnel, other than during training, will be reported to the Project Manager or Team Supervisor. The incident will also be reported to the Participating Agency according to its agency policy.

V. **INVESTIGATIVE AND EVIDENTIARY PROCEDURES**

- A. No Superseding Standard of Care, Duty or Conduct. Nothing in the SOP or any policy, procedure, practice, protocol or guideline resulting therefrom is intended to alter or affect, or does alter or affect, any standard of care, standard of conduct, or lawful authority to search, seize or arrest under the Constitution of the United States, any federal or state law or international treaty or its equivalent, or any policy or procedure of the FBI or any other law enforcement entity.
- B. Applicable Investigative Legal Process. The selection of applicable legal process to facilitate CCTF investigations (e.g., search warrants, administrative or grand jury subpoenas, pen register or trap and trace orders, intercept orders and consensual monitoring documentation requirements) shall be designated by the FBI Program Manager or the Team Manager in consultation with appropriate prosecutive agencies.
- C. Report Format. In order to facilitate the national sharing of information, all Participating Agency personnel shall prepare written reports in compliance with the format and manner utilized by the FBI. Any exceptions to this general requirement must be approved in advance by the Program Manager. In addition, only one evidentiary document, such as a report of investigation, will be prepared in joint investigations.
- D. FBI Databases and Information Systems. All reports shall be uploaded into applicable FBI databases or information systems so that information sharing is enhanced between task forces and other law enforcement investigators.
- E. Ownership and Retention of Information.
  1. Any records developed in an investigation in which the FBI is a participant will be considered exclusively FBI records, although copies may be loaned to other Task Force Participating Agencies subject to law, regulation, and policy.
  2. Records developed in investigations in which the FBI is not a participant will be owned and retained as agreed upon by the relevant Participating Agencies.
  3. Administrative records of the CCTF, and CCTF records that are not otherwise owned by another Participating Agency, also will be considered exclusively FBI records and similarly may be loaned to other Task Force Participating Agencies subject to law, regulation, and policy.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*



4. FBI records and information shall not, if provided to a State or local government Participating Agency, be made available pursuant to any State or local law requiring disclosure of information or records. Rather, any requests to a State or local government Participating Agency for any FBI or other Federal government records or information shall be referred to the FBI for proper handling.

F. Forensic Examination Procedures.

1. Forensic Examinations are Restricted to CCTF Evidence. The mission of the CCTF is investigative and not forensic. Any forensic acquisition and examination of evidence must be authorized by the Program Manager, and shall only be conducted on evidence from an investigation initiated or adopted by the CCTF.
2. Procedures for Handling Digital Evidence Generated by CCTF-Initiated Investigations. Digital evidence accepted, seized, acquired or intercepted by the CCTF pursuant to a criminal investigation initiated or adopted as a CCTF investigation, shall be forensically examined only when expressly authorized by the Program Manager and only as follows:
  - a. By any assignee to the CCTF who:
    - (1) is affiliated with, certified, and monitored or supervised by an established and recognized crime "laboratory" of his or her respective Participating Agency; and
    - (2) conducts such examination in conformity with the written protocols, policies and procedures of such laboratory;
  - b. By any non-CCTF personnel belonging to the criminal laboratory of a Participating Agency who:
    - (1) is affiliated with, certified, and monitored or supervised by an established and recognized crime "laboratory" of a Participating Agency; and
    - (2) conducts such examination in conformity with the written protocols, policies and procedures of -- and onsite at -- the Participating Agency's laboratory;
  - c. By FBI personnel who:
    - (1) are FBI Computer Analysis Response Team (CART) trained and certified (or otherwise are trained and certified in a manner expressly accepted by CART), and will conduct such examination in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of FBI CART; or,
    - (2) are FBI Forensic Audio/Video Image Analysis Unit (FAVIAU) trained and certified and will conduct such examinations in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of FBI FAVIAU; or,
  - d. Any FBI CART trained and certified personnel (or personnel otherwise trained and certified in a manner expressly accepted by CART) assigned to an FBI-Affiliated Regional Computer Forensic Laboratory (RCFL) who will conduct such examinations in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of that RCFL.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

3. Definition of the term "Laboratory." For purposes of inclusion but not exclusion under this section, a "laboratory" shall be considered established and recognized if it has become accredited in digital evidence examinations by the American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD-LAB).
4. Digital Evidence Generated by FBI-Initiated Investigations. Digital evidence accepted, seized, acquired or intercepted by FBI personnel which, at the time of its acceptance, seizure, acquisition or interception related to a non-CCTF designated, FBI-initiated investigation shall be forensically examined by FBI personnel who:
  - a. Are FBI Computer Analysis Response Team (CART) trained and certified, and will conduct such examination in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of FBI CART, or
  - b. Are FBI Forensic Audio/Video Image Analysis Unit (FAVIAU) trained and certified and will conduct such examination in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of FBI FAVIAU, or
  - c. Are otherwise expressly authorized in advance by an appropriate FBI Program Manager of the FBI Investigative Technology Division.
5. FBI Digital Forensic Examinations Conducted Only Pursuant to FBI CART Procedures and Protocols. All digital evidence examinations on either CCTF or FBI-initiated or adopted investigations which are conducted by FBI personnel shall be:
  - a. conducted by FBI CART trained and certified personnel in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of FBI CART, unless otherwise expressly authorized in writing by FBI-HQ CART, or
  - b. in the case of digital audio/ video / image forensic analysis, by FBI FAVIAU trained and certified personnel who will conduct such examinations in conformity with the written Standard Operating Protocols and Quality Assurance Manual requirements of FBI FAVIAU.
6. Evidence Storage. The FBI Program Manager may designate a volunteering Participating Agency to exercise control over some or all of the evidence gathered by and in the course of CCTF investigations and, thereafter, the rules and policies of that Participating Agency relating to the submission of evidence, retrieval, destruction and chain of custody shall apply. In the absence of a designation, the FBI shall exercise control over all such evidence and its rules and policies shall apply.

## VI. ADMINISTRATIVE PROCEDURES

- A. Cross-deputation of Sworn Personnel
  1. Definition of the term "Sworn Law Enforcement Assignee." For purposes of this SOP, "sworn law enforcement assignees" means those state and local law enforcement officers authorized by law to enforce criminal statutes and judicial sanctions (including the power to investigate, and arrest), and who are authorized to carry a firearm and exercise appropriate force (including deadly force) in the lawful exercise of those duties.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

2. Federal Deputation of Sworn Law Enforcement Assignee: In limited circumstances and subject to the successful completion of additional documentation and agreements (including non-disclosure agreements), background investigation inquiries and security clearances as may be deemed appropriate, State Executive Agency (SEA) "sworn law enforcement assignees" may be federally deputized for the limited purpose of providing direct support to the CCTF. The FBI or another Federal Executive Agency (FEA) shall coordinate the securing of the required deputation authorizations. These deputations may remain in effect throughout the tenure of each individual's assignment to the CCTF, as limited by the terms of the deputation or until termination of the relationship between the FBI or other FEA and the CCTF or the termination or dissolution of the CCTF itself, whichever comes first. Administrative and personnel policies imposed by the Participating Agencies will not be voided by deputation of their respective sworn personnel. Any federal law enforcement powers authorized under any federal deputation program shall be suspended upon the suspension of any state, local or municipal law enforcement authority.
3. State Deputation of Federal Sworn Personnel: In limited circumstances and subject to the successful completion of additional documentation and agreements (including non-disclosure agreements), background investigation inquiries, FBI and other FEA agents may be cross-deputized as state peace officers with state law enforcement authority. These deputations may remain in effect throughout the tenure of each individual's assignment to the CCTF, as limited by the terms of the deputation or until termination of the relationship between the FBI or other FEA and the CCTF or the termination or dissolution of the CCTF itself, whichever comes first. Administrative and personnel policies imposed by the Participating Agencies will not be voided by deputation of their respective sworn personnel. For purposes of this SOP, any state law enforcement powers authorized under any state deputation program shall be suspended upon the suspension of the CCTF member's separation from the CCTF for any reason.

B. Intergovernmental Personnel Act Assignments to Federal Agencies

1. SEA Personnel May Be Formally Detailed to the FBI or Another FEA and Thereafter Assigned to the CCTF. Subject to approval by the affected FEA and SEA, any SEA employee, including but not limited to administrative support personnel, assigned to the CCTF may seek to be formally "detailed" to the FBI or another FEA as a civilian employee pursuant to the Intergovernmental Personnel Act (IPA), 5 U.S.C. §3374, and thereafter be assigned by the FBI or other FEA to the CCTF. Thereafter, during the period of the detail and pursuant to 5 U.S.C. §3374(c)(2), such an employee acting within the scope of their assignment shall be entitled to all of the rights, privileges and immunities accorded by law including being "deemed an employee of the [FEA] for the purpose of .... the Federal Tort Claims Act and any other Federal tort liability statute." The FEA accepting the "detailed" employee shall be presumed to have accepted the SEA employee under an agreement not requiring reimbursement from the FEA to the SEA of compensation (which shall continue to be paid by the SEA to the employee during the period of the detail). The failure to be formally detailed pursuant to the IPA to an FEA for purposes of assignment to the CCTF shall not prohibit any SEA Participating Agency

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

from offering to assign an employee to the CCTF and shall not prejudice the rights of such a SEA employee (as described in other provisions of this SOP) to seek legal representation, substitution and/or indemnification from the Federal government for acts or omissions occurring pursuant to and within the course and scope of their assigned duties while assigned to the CCTF.

2. Employees of Institutions of Higher Education and "Other Organizations" May Be Formally Detailed to the FBI or Another FEA and Thereafter Assigned to the CCTF. Any employee of an Institute of Higher Education (IHE), or an "other organization" (OO) as defined by 5 U.S.C. §3371(4), possessing the knowledge, skills or ability necessary to facilitate the mission of the CCTF may seek to be formally "detailed" to the FBI or another FEA pursuant to the Intergovernmental Personnel Act (IPA), 5 U.S.C. §§3372(b)(2) & (e)(2), and thereafter be assigned by the FBI or other FEA to the CCTF in a civilian support role. During the period of the detail, pursuant to 5 U.S.C. §3374 (c)(2) such an employee acting within the scope of their assignment shall be entitled to all of the rights, privileges and immunities accorded by law including being "deemed an employee of the [FEA] for the purpose of .... the Federal Tort Claims Act and any other Federal tort liability statute." An employee detailed pursuant to the IPA shall be presumed to be accepted under an agreement not requiring reimbursement from the FEA to the IHE or OO of compensation (which shall continue to be paid by the IHE or OO to the employee during the period of the detail).

C. Personnel Administrative Issues

1. FEA Personnel Generally Shall Not be Deemed SEA Personnel. Except as expressly authorized in a separate writing pursuant to an established state, local or municipal deputation program for sworn personnel, or the IPA for non-civilian support personnel, FEA personnel, including FBI personnel, assigned to the CCTF shall not be deemed employees of any SEA for any purpose merely by virtue of their assignment to the CCTF.
2. SEA Personnel Generally Shall Not be Deemed FEA Personnel. Except as expressly authorized in a separate writing pursuant to an established federal deputation program for sworn personnel, or the IPA for non-civilian support personnel, SEA personnel detailed to the CCTF shall not be deemed employees of the FBI or the United States of America for any purpose merely by virtue of their detail to the CCTF.
3. No CCTF Employees. The CCTF is not a separate legal entity capable of maintaining an employer-employee relationship and, as such, all personnel detailed to the CCTF shall NOT be considered employees of the CCTF for any purpose.
4. Duration of CCTF Detail by Participating Agencies. Except for personnel assigned to the CCTF to perform purely administrative functions, each Participating Agency generally shall offer for assignment to the CCTF the full-time services of not less than one (1) of its respective personnel (acceptable for detail by the CCTF) to serve for a period of at least one year, renewable annually thereafter.
5. Training Opportunities. Pursuant to 42 U.S.C. §3771(a) and 28 C.F.R. §0.85 and other legal authority, the FBI may, in its discretion and subject to available funding, offer, at FBI expense, such training and educational opportunities as may be appropriate.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

Training by other law enforcement entities, private vendors, and educational institutions also may be made available for CCTF assignees pursuant to training needs and available funding.

6. Conflicts of Interest. Personnel assigned to the CCTF may not engage in any activity which, either in appearance or in fact, conflicts with their duties at the CCTF or reasonably impeaches the independence of their work for the CCTF. Except upon the express approval of the FBI Program Manager or the Team Manager no assignee shall act as a consultant regarding computer crime either for free or for profit or remuneration beyond the salary paid by their employing agency during the period of their detail to the CCTF. CCTF assignees shall not endorse any hardware, software, or other product, on behalf of the CCTF or in their capacity as a member of the CCTF.
7. CCTF Assignees Continue to Periodically Report to Their Employers. Each CCTF assignee will continue to report periodically to his or her respective agency supervisor or CEO for administrative matters unrelated to the case-specific assignments of the CCTF which are not otherwise specifically described in this SOP.
8. CCTF Not to Conduct Performance Appraisals. Performance appraisals of personnel detailed to the CCTF shall not be conducted by the FBI Program Manager or the Team Manager on behalf of that employee's Participating Agency unless the FBI Program Manager or the Team Manager is otherwise an assignee of the same Participating Agency as the personnel under performance review, except that the FBI Program Manager or the Team Manager may, at the written request of an appropriate rating official, provide written comments for possible use by that official regarding performance related issues/appraisals.

D. Personnel Financial Issues:

1. Employment-related Expenses of Personnel Assigned to the CCTF. Participating agencies shall bear all personnel costs for any personnel detailed to the CCTF including but not limited to salaries, benefits, employment taxes, withholdings, travel expenses, insurance, retirement expenses, disability and all other employment-related benefits incident to their employment with their respective agencies.
2. Travel Expenses Incurred on Behalf of the CCTF. Assignees must receive written pre-approval by the reimbursing entity for all travel expenses incurred on behalf of the CCTF. Subject to funding availability, any Participating Agency may, in its discretion, pay travel costs for out-of-state travel of CCTF assignees, should the Participating Agency deem such travel necessary, provided that the fact of such a payment in any one instance or number of instances shall not create or support any duty or obligation to make future payments unless otherwise agreed to in writing.
3. Overtime and other Compensation for CCTF Assignees. Compensation for overtime, holiday pay, vacation, and sick leave, shall be the responsibility of each Participating Agency with respect to their assigned employee(s). It shall be the joint responsibility of each Participating Agency and its assigned employee to regularly and timely inform the FBI Program Manager or the Team Manager of available overtime, scheduled vacation, annual leave or sick leave. Participating Agencies may, in their discretion, delegate to the FBI Program Manager or the Team Manager limited authorization to schedule their

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

detailed employee(s) for overtime or holiday pay or other applicable compensation as may be necessary to effectuate the purpose and mission of the CCTF. The FBI Program Manager or the Team Manager shall coordinate with the Participating Agencies, if and when alternate funding is available, for the payment or reimbursement of overtime or other compensation provided that the fact of such a payment in any one instance or number of instances shall not create or support any duty or obligation to make future payments unless otherwise agreed to in writing.

4. Participating Agencies to Supply Their Assignees with Communication Devices. Except as otherwise agreed to in writing, each assignee will be provided a cell phone and/or pager by the assignee's Participating Agency to ensure communication capabilities with the CCTF.
5. Grievances, Complaints, Discipline.
  - a. Employee Rights Unaffected by Assignment to CCTF/Remedies with Assigning. Because FEA assigned personnel are not employees of the CCTF or of any of the SEAs and, similarly, because SEA assigned personnel are not employees of the CCTF or of any of the FEAs, the substantive and procedural rights of such personnel regarding employment-related grievances or discipline are governed solely by the contracts, rules and regulations existing between the assigned personnel and their respective employing agencies. Assignment to the CCTF creates no legally enforceable rights in such personnel to the continuation of the assignment to the CCTF or otherwise.
  - b. SEA Assignees Shall Voluntarily Consent to Assignment. SEA personnel may not be assigned to the CCTF unless they voluntarily consent prior to the detail. Upon detail to the CCTF, SEA assignees shall be provided a copy of this SOP and any related MOU by the Program Manager or Team Manager. The Program Manager shall maintain a record that he or she provided each assignee with this SOP and any related MOU. It shall be the duty of all SEA assignees to promptly notify the Program Manager in writing within seven (7) days of provision of this SOP if such assignee does not voluntarily consent to the assignment and the terms of this SOP and any related MOU, in which case the assignee shall return to his or her Participating Agency.
  - c. No CCTF-vested Rights. There shall be no disciplinary or grievance procedure, policy or process within the CCTF which will vest any rights in any CCTF assigned personnel, FBI Program Manager, or Team Manager, and all Participating Agencies and their assignees agree that no alleged procedure, policy, process or practice shall be relied upon or be binding upon the Participating Agencies or their assigned personnel.
  - d. Application of Grievance Procedures. Any CCTF assignees with complaints, suggestions, comments or concerns regarding the policies, procedures, practices or decisions of the FBI Program Manager or the Team Manager are strongly encouraged, but not required, to first informally discuss such matters with the FBI Program Manager or the Team Manager. Any CCTF assignee who is unsatisfied with CCTF policies, procedures, practices or decisions may refer the matter to his or her employing agency for processing pursuant to that agency's grievance procedure, the sole remedy for which (as enforceable against the

CCTF) shall be the discontinuance of the assignee's assignment to the CCTF and his or her return to his or her employing agency.

- e. Grievances Initiated by CCTF Personnel/ CCTF Response. In the event that a CCTF assignee refers a matter to his or her employing agency for appropriate grievance processing, the Participating Agency shall, to the maximum extent possible, inform the FBI Program Manager or the Team Manager of the nature and circumstances of the grievance and the agency's grievance procedure as permitted or authorized by that participating agency's regulations, policies, practices, employee related contractual agreements or consent of the complainant. The Participating Agency shall order the temporary return of the grieving assignee to his or her employing agency during the pendency of the grievance procedure unless otherwise agreed to by the FBI Program Manager or the Team Manager. The Participating Agency shall, at the conclusion of the grievance procedure, inform the FBI Program Manager or the Team Manager of the grievance findings and/or recommendations, if any. The FBI Program Manager or the Team Manager are not bound by any such final or intermediary decision of any SEA or FEA grievance procedure and are not required to implement any final or intermediary grievance recommendation. However, the FBI Program Manager or the Team Manager may, in their discretion, consider incorporating or adopting all or part of any agency's grievance recommendation. All Participating Agencies shall insure that discontinuance of an assignment to the CCTF following an assignee-initiated grievance procedure SHALL NOT be considered or interpreted as discipline or otherwise negatively affect or reflect upon that person's performance while assigned to the CCTF.

- f. Reports of Assignee Misconduct or Unsatisfactory Performance by FBI Program Manager or the Team Manager to Participating Agencies for Possible Discipline. In any instance in which an assignee, in the judgment of the FBI Program Manager or the Team Manager, may have engaged in misconduct or failure to fulfill the mission or purpose of the CCTF as requested, the FBI Program Manager or the Team Manager shall notify the Participating Agency of the assignee's employing agency in writing of the details of the alleged misconduct or failure. The notification shall carry no greater weight or effect than any other complaint by another law enforcement agency. The Participating Agency shall then take such steps as it deems appropriate in conformity with the statutory or contractual obligations, policies, procedures and/or practices of that agency. The Participating Agency shall order the temporary return of the assignee to their employing agency during the pendency of that agency's disciplinary or review process unless otherwise agreed to by the FBI Program Manager or the Team Manager. At the conclusion of the disciplinary procedure of the employing agency, the Participating Agency shall notify the FBI Program Manager or the Team Manager of the employing agency's findings, decisions, and/or actions, if any. The FBI Program Manager and the Team Manager may or may not, in their independent judgment and discretion, accept the findings, decisions, and/or action of the assigning agency. In the event that conduct is found by the employing agency not to constitute misconduct or any violation

requiring any action, but the FBI Program Manager or the Team Manger nonetheless elects to discontinue the assignment to the CCTF, the discontinuance of the assignment shall not be considered or interpreted as discipline or otherwise negatively affect or reflect upon that person's performance while assigned to the CCTF. The CCTF is not bound by any final or intermediary disciplinary decision of an employing agency, EXCEPT that the FBI Program Manager or the Team Manager is bound by and shall honor any agency decision or ruling suspending from employment or otherwise suspending the law enforcement powers of any employee. Any federal law enforcement powers authorized under any federal deputation program shall be suspended upon the suspension of any state, local or municipal law enforcement powers.

## VII. NON-DISCLOSURE OF INFORMATION/MEDIA POLICY

- A. Non-Disclosure Agreement. CCTF assignees agree not to disclose any classified or otherwise sensitive case information to non-CCTF assignees (to include an assignee's employing Participating Agency) without the express permission of the FBI Program Manager or his designee and shall agree to execute any applicable non-disclosure agreements, including SF-312 and FD-868, as may be necessary or required by the FBI. To the extent current or former CCTF assignees desire to disclose outside of their official investigative duties (including, but not limited to, for purposes of teaching or within a fiction or non-fiction book) -- any information acquired from or relating to their CCTF participation, they will do so only with advance written permission and in compliance with the FBI's prepublication review procedures. CCTF assignees have a continuing obligation after leaving the CCTF to maintain their non-disclosure commitment. If assignees have access to Title III, FISA, federal grand jury, or other information subject to statutory or court-imposed restrictions, the assignee will be briefed by the FBI on his or her responsibilities under any applicable statutes, court orders, or minimization procedures. Participating Agencies and assignees agree to be bound by all CCTF policies on the disclosure of information, and agree to consult with the FBI prior to any such disclosure during or after the assignment. The assignee is encouraged to seek authorization to disclose information whenever he or she believes disclosure would be appropriate.
- B. Media Inquiries Referred to the FBI Program Manager or the Team Manager. All media inquiries are to be referred to the FBI Program Manager or the Team Manager. The FBI Program Manager or the Team Manager or his/her designee may comment to the media upon the general operation of the CCTF and the participation of the member agencies and departments after consultation with the appropriate Participating Agency(ies). Where the inquiry is case specific, comments, if any, will be left to the discretion of the submitting law enforcement agency. In the case of the public release of information by a Department of Justice employee or information relating to a case or matter investigated or prosecuted by the Department of Justice, the release of such information shall comply with the requirements of 28 C.F.R. §50.2.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*



## VIII. FINANCIAL AND CIVIL LIABILITIES IN GENERAL

- A. Federally Deputized Personnel. The Participating Agencies and their assignees acknowledge that financial and civil liability, if any and in accordance with applicable law, for the acts and omissions of each assignee committed in conjunction with or during assignment to the CCTF remains vested with the assignee's employing agency. However, the United States Department of Justice may, in its discretion, formally determine that an individual should be afforded a legal defense and/or indemnification pursuant to federal law and the policies of the Department of Justice, for instance to:
1. those sworn law enforcement officers who have been properly federally deputized by an FEA and are acting within the scope and course of their deputation and their duties as provided by Federal law; and
  2. those employees formally detailed to a FEA pursuant to 5 U.S.C. §3374 (the Intergovernmental Personnel Act of 1970);
- B. Federal Tort Claims Act. Congress has provided that the exclusive remedy for the negligent or wrongful act or omission of an employee of the United States government, acting within the scope of his/her employment, shall be an action against the United States under the Federal Tort Claims Act (FTCA), 28 U.S.C. § 1346(b), §§ 2671-2680.
- C. "Employee" of the United States. For the limited purpose of defending claims arising out of a CCTF in which the FBI is a Participating Agency: Those State or local law enforcement officers who have been federally deputized, and those State and local personnel who have been formally detailed to the FBI or any other FEA pursuant to 5 U.S.C. §3374, and who are acting within the course and scope of his or her official duties, details, and assignments pursuant to this SOP, may be considered an "employee" of the United States government as defined in 28 U.S.C. § 2671. See 5 U.S.C. § 3374(c)(2).
- D. Scope of Employment. Under the Federal Employees Liability Reform and Tort Compensation Act of 1988 (commonly known as the Westfall Act), 28 U.S.C. § 2679(b)(1), the Attorney General or his/her designee may certify that an individual defendant acted within the scope of his/her employment at the time of the incident giving rise to the suit. Id., 28 U.S.C. § 2679(d)(2). The United States can then be substituted for the employee as the sole defendant with respect to any tort claims. 28 U.S.C. § 2679(d)(2). If the United States is substituted as a defendant, the individual employee is thereby protected from suits in his/her official capacity.
- E. Petition for Scope of Employment Designation. If the Attorney General declines to certify that an employee was acting within the scope of employment, "the employee may at any time before trial petition the court to find and certify that the employee was acting within the scope of his/her office or employment." 28 U.S.C. § 2679(d)(3).
- F. Liability. The Participating Agencies do not waive, and intend to assert, available liability limitations in all cases. Unless otherwise indemnified or immune, each Participating Agency shall assume the responsibility and liability for the acts and omissions of its own officers, agents, or employees in connection with the performance of their office duties. For tort liability purposes,

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

no Participating Agency shall be considered the agent of the other Participating Agencies. Each Participating Agency shall be liable (if at all) only for the torts of its own officers, agents, or employees that occur within the scope of their official duties.

- G. Bivens Actions. Liability for violations of federal constitutional law rests with the individual Federal agent or officer, or employee, pursuant to Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) or pursuant to 42 U.S.C. § 1983 for State and local officers or cross-deputized Federal officers.
- H. Indemnification. If a federally deputized officer or an employee formally detailed to an FEA pursuant to 5 U.S.C. §3374 is found to be liable for a constitutional tort, he/she may request indemnification from DOJ to satisfy an adverse judgment rendered against the employee in his/her individual capacity. 28 C.F.R. § 50.15(c)(4). The criteria for indemnification are substantially similar to those used to determine whether a Federal employee is entitled to DOJ representation under 28 C.F.R. § 50.15(a).
- I. Qualified Immunity. Both state and federal officers enjoy qualified immunity from suit for constitutional torts "insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." Harlow v. Fitzgerald, 457 U.S. 800 (1982).
- J. Representation. CCTF personnel may request representation by the U.S. Department of Justice (and subject to its determination) for civil suits against them in their individual capacities for actions taken within the scope of employment. 28 C.F.R. §§ 50.15, 50.16.
1. An "employee" may be provided representation "when the actions for which representation is requested reasonably appear to have been performed within the scope of the employee's employment and the Attorney General or his/her designee determines that providing representation would otherwise be in the interest of the United States." 28 C.F.R. § 50.15(a).
  2. A CCTF assignee's written request for representation should be directed to the Attorney General. In the case of officers federally deputized through the FBI, or detailed to the FBI pursuant to 5 U.S.C. §3374, written requests should be provided to the Chief Division Counsel (CDC) of the FBI division participating in the CCTF. The CDC will then forward the representation request to the FBI's Office of the General Counsel (OGC) together with a Letterhead Memorandum concerning the factual basis for the lawsuit. FBI/OGC will then forward the request to the Civil Division of DOJ together with an agency recommendation concerning scope of employment and Department representation. 28 C.F.R. § 50.15(a)(3).
- K. Notification of Claims. The Participating Agencies agree to notify each other of any claim or law suit arising out of an activity conducted pursuant to this SOP or the related MOU. Nothing in this paragraph shall prevent any Participating Agency made a party to or affected by any claim or law suit from conducting an independent administrative review of any matter giving rise to the claim or lawsuit. All Participating Agencies agree to cooperate fully with one another in the event

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

of an administrative review or official investigation of alleged negligence or misconduct arising out of activity conducted pursuant to this SOP or the related MOU. Nothing in this paragraph shall be construed as supplanting any applicable statute, rule, or regulation.

## IX. VEHICLES, EQUIPMENT, PROPERTY, AND GIFTS

### A. Vehicles.

1. Participating Agencies to Supply Their Assignees with Vehicles. Transportation, both to and from the CCTF and in support of the mission and operational requirements of the CCTF, will be the responsibility of and provided in accordance with the policies and procedures of the assignee's employing agency. Except as provided in subparagraph IX.A.2 below, each Participating Agency agrees to defend, indemnify, and hold all other Participating Agency members from any claims or liability arising out of the use of the former's vehicles.
2. FBI Vehicles. On a case-by-case basis, and as may be subject to a separate vehicle use agreement, an FBI division may authorize State or local law enforcement personnel assigned to the CCTF to use (operate or be transported in) available vehicles owned or leased by the FBI when necessary and in direct support and in connection with the official business of the CCTF. When such vehicle use is authorized, the employing Participating Agency agrees to be responsible for, defend, indemnify, and hold the FBI and the United States harmless for any claims or liability resulting from its assignee's use of the FBI owned or leased vehicles, and for any damage to said vehicles or to CCTF assignees or third parties as a result of any action or omission on the part of the Participating Agency or their employees. When authorized, CCTF assignees using FBI vehicles agree to operate the vehicles in accordance with all applicable FBI rules and regulations as outlined in the FBI Manual of Administrative Operations and Procedures (MAOP), Part I, Section 3.1.

### B. Property of Participating Agencies Terminating Their Relationship with the CCTF.

Equipment and other tangible property, excluding monies, provided by Participating Agencies will remain the property of each agency and will be retrieved by that agency within ninety (90) days of the termination of that agency's relationship with the CCTF, unless otherwise agreed to in writing. Equipment and other tangible property not so retrieved shall be deemed abandoned property transferred in title to the FBI for the collective benefit of the CCTF Participating Agencies until termination of the CCTF.

### C. Certain Tangible Properties & Monies Acquired for CCTF Use. Unless otherwise directed by the FBI, or mandated by applicable law, the following tangible property and monies -- where acceptance is authorized -- shall be used for the collective benefit of active CCTF Participating Agencies during the existence of the CCTF:

1. Tangible and intangible property and/or monies forfeited to any Participating Agency primarily as a result of services rendered by the CCTF;
2. Tangible and intangible property and/or monies obtained through a grant by or for the CCTF; and,

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

3. Tangible and intangible property and/or monies expressly donated to or for the CCTF.
- D. Intellectual Property. Intellectual Property rights generated, in whole or in part, by or as a consequence of the operations of the CCTF shall be governed as follows:
1. All patentable rights generated by 1) FEA personnel, 2) personnel assigned to an FEA pursuant to 5 U.S.C. § 3374, and/or 3) SEA sworn law enforcement personnel who have been federally deputized and assigned to the CCTF, shall be the property of the United States Government, the disposition of which shall be governed by Executive Order 10096, or its successor, and 37 C.F.R., Part 501 as may be amended.
  2. All patentable rights generated by any non-for-profit organization or small business which were funded, either in whole or in part, under grants, contracts or cooperation agreements with the United States Government shall be controlled by and disposed of pursuant to 37 C.F.R., Part 401.
  3. All other intellectual property rights and interests generated in whole or in part by the CCTF assignees, or otherwise generated in whole or in part through the use of equipment or property granted, purchased, donated, forfeited or abandoned to or for the benefit of the CCTF shall transfer to or be titled in the name of the United States Government for the collective benefit of the CCTF Participating Agencies and shall be controlled by the United States Government, except that intellectual property rights in educational texts, journals, or treatises of assignees which have been subject to pre-publication review and approval shall not, in the absence of a specific directive by the FBI, inure to the benefit of the CCTF, but instead shall be governed by the policy of the assignee's Participating Agency, if any.
- E. Educational Texts & Journals of Assignees. Except as authorized by the FBI Program Manager or the Team Manager, no assignee shall disseminate to the public at large (during the existence of the CCTF) any text, journal, treatise or other material relating to the investigation or prosecution of cyber crime or the collection, acquisition and/or interception and examination of digital evidence which discusses or discloses any investigative information, or any policy, practice, or procedure used by the CCTF or any of its Participating Agencies, past or present, which has not clearly been identified as authorized for public dissemination, or has otherwise not been made public. Nor shall any assignee disclose his or her present affiliation with the CCTF except in accordance with 5 C.F.R. §2635.807(b) in a manner approved by the FBI Program Manager or the Team Manager.
- F. Assumption of Risk of Loss of Agency Property. Each Participating Agency agrees to assume the risk of and financial responsibility for damage to or loss of its property as a result of its use by or in conjunction with CCTF operations.
- G. Operational Supplies/Equipment. Office supplies, equipment, furniture and other property necessary to operate the CCTF shall be provided to the CCTF by Participating Agencies and/or be purchased through available funds by the FBI Program Manager or, as separately authorized, by the Team Manager or his/her designee.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

- H. Gifts by Non-Governmental, Non-Participating Entities. Neither the CCTF, any Participating Agency, nor any assignee to the CCTF may solicit or accept any monies, or any tangible or intangible property or services without just compensation in exchange therefor, for the benefit of any Department of Justice Participating Agency or assignees of /detailees to such a DOJ Agency from any non-Participating Agency or non-governmental entity or person, except that:
1. Nothing in this provision shall prohibit the solicitation, temporary or incidental acceptance of information or software from any person as may be necessitated by the need to conduct an analysis of evidence in a case-specific matter;
  2. Nothing in this provision shall prohibit the solicitation or acceptance of any technical training offered to all law enforcement which is not promotional in nature and may be solicited or accepted in accordance with applicable rules, regulations and laws;
  3. Nothing in this provision shall prohibit any SEA, acting in accordance with its applicable rules, regulations and laws, from soliciting or accepting on behalf of any SEA any property, monies or services for the benefit of the SEA, or fellow SEAs, regardless of whether such property, monies or services shall be used by personnel assigned to the CCTF, provided that:
    - a. Title to property so solicited and/or accepted shall not pass to a Federal agency; and,
    - b. The origin of property so solicited and/or accepted during the existence of the CCTF shall be disclosed to the FBI Program Manager or the Team Manager if it is used by the CCTF generally or is made available to all assignees;
  4. Nothing in this provision shall prohibit the acceptance or solicitation of any gift by any Federal agency in accordance with 28 U.S.C. § 524(d)(1) and applicable DOJ orders, or any amendments thereto or other lawful authority. All DOJ entities and their assignees/detailees shall, at all times, comply with 5 C.F.R. 2635.201 et. seq. as well as any rules and regulations of their respective agencies.

X. **COSTS.** Unless otherwise provided herein or in a supplementary writing, each Participating Agency shall bear its own costs in relation to this SOP and any related MOU. Even where a party has agreed (or later does agree) to assume a particular financial expense, the party's express written approval must be obtained before the incurring by another party of such expense. All obligations of and expenditures by the parties will be subject to their respective budgetary and fiscal processes and availability of funds pursuant to all laws, regulations, and policies applicable thereto. The parties acknowledge that there is no intimation, promise, or guarantee that funds will be available in future years.

XI. **NO THIRD PARTY RIGHTS.** This SOP is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties to any related MOU, the CCTF, any CCTF Participating Agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

## XII. MODIFICATIONS AND AMENDMENTS

- A. Modifications/amendments to this SOP shall be brought to the attention of each Participating Agency.

Official Law Enforcement Use Only

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

- B. Participating Agencies and their assignees are bound by the terms of this SOP, as modified from time to time, although a Participating Agency may terminate its participation with the CCTF pursuant to the terms of the related MOU.
- C. Participating Agency will not be considered bound by any amended terms of the SOP during any notice period (currently 30 days) required by the MOU prior to terminating participation.

### **XIII. LEGAL CONSTRUCTION AND SEVERABILITY**

- A. If any portion of this SOP or a related MOU is declared invalid by a court of competent jurisdiction, this SOP shall be construed as if such portion had never existed, unless such construction would constitute a substantial deviation from the intent of the Participating Agencies as reflected in this SOP or a related MOU.
- B. If any portion of this SOP or any related MOU are found to be in conflict, the MOU shall be deemed to control.

xxxx  
end.

**Official Law Enforcement Use Only**

Cyber Crime Task Force  
Standard Operating Procedures (June 2004)

*This document contains neither recommendations nor conclusions of the FBI. This document is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.*

**City of Saint Paul Financial Analysis**

1 File ID Number: RES PH 11-1103  
2  
3 Budget Affected: Operating Budget Police Department Special Fund  
4  
5 Total Amount of Transaction: \$5,000.00  
6  
7 Funding Source: Grant  
8  
9 Charter Citation: 10.07.1  
10  
11

12 Fiscal Analysis

13  
14  
15 WHEREAS, the City of Saint Paul, Police Department is authorized to enter Memorandum of Agreement  
16 with the FBI to be reimbursed for expenditures and equipment purchased for the MCCTF not to exceed  
17 \$5,000.  
18  
19  
20  
21  
22  
23  
24  
25  
26

27 Detail Accounting Codes:  
28  
29

Company (Fund)	Accounting Unit (ACTIVITY)	Account (Object Code)	Description	CURRENT BUDGET	CHANGES	AMENDED BUDGET
<b>Spending Changes</b>						
1000 (001)	10004229 (04229)	54190 (0370)	Computer	-	5,000	5,000
				TOTAL:	0	5,000
<b>Financing Changes</b>						
1000 (001)	10004229 (04229)	42920 (4398)	Services - Special Projects	-	5,000	5,000
				TOTAL:	0	5,000

30  
31  
32  
33  
34  
35  
36  
37  
38