

Instructor Development Policy and Guidelines

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-17-2011 BY 65179 DMH/STW



Federal Bureau of Investigation
Training Division
FBI Academy

POL[YR]-[00XX]-TD

[DRAFT]
FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041866

FBI040766

GENERAL INFORMATION: Questions or comments pertaining to the Instructor Development Policy and Guidelines can be directed to:

FBI HQ/Training, Division [02]

Resource Management Section, Strategic Planning and Policy Unit

Division Point of Contact: Federal Law Enforcement Training Accreditation (FLETA) Office of Accreditation:

b6
b7C

(Note: Document is a new publication; no previous versions are available)

PRIVILEGED INFORMATION

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041867

FBI040767

Instructor Development Policy and Guidelines

Table of Contents

1. Scope.....	4
2. Policies Regarding Instructional Certification.....	4
3. Training Development, Responsibilities and Requirements.....	5
3.1 Instructor Requirements.....	5
3.2 Instructor Development and Responsibilities.....	6
3.3 Providing Instructor Development Training.....	8
4. Criteria for Successful Completion of Instructor Training.....	9
5. Instructor Mentoring, Evaluation and Remediation.....	10
6. Recordkeeping Requirements.....	10
7. Document Control.....	10
7.1 Lesson Plan Approval and Issuance.....	11
7.2 Revisions to Instructional Material.....	12
7.3 Responsibilities.....	13
7.4 Lesson Plan Formatting.....	13
8. Training Requested or Provided by Outside Entities.....	14
9. Use of Licensed and Copyrighted Material.....	15
10. Safety Considerations and Risk Assessments.....	15

List of Appendices

Appendix A: Definitions and Acronyms

Appendix B: Sources of Additional Information

Appendix C: Forms

Appendix D: Revision History and Approval and Issuance

[DRAFT]
FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

Federal Bureau of Investigation

Instructor Development Policies and Guidelines

1 Scope

Purpose: These policies and guidelines will be set forth to assist with the process of providing instructors with the training and skills required to successfully provide instruction to New Agent Trainees, National Academy students, Center of Intelligence Training, and other Law Enforcement entities.

Background: In order to be successful in the accreditation endeavor, the Training Division (TD) Federal Law Enforcement Training Accreditation (FLETA) Office of Accreditation has established policies and guidelines for ensuring instructor development within the FBI. Upon receiving FLETA accreditation, the Training Division will continue to demonstrate its adherence to quality, effectiveness and integrity.

Intended Audience: These policies and guidelines are intended to assist all TD instructional personnel.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041869

FBI040769

2 Definitions

Academy - is a designated training organization, including staff, facilities, etc., that conduct basic or specialized/advanced law enforcement training for Federal law enforcement personnel.

Adjunct Instructor - is an individual who has a high level of subject matter expertise that exceeds the requirement for the FBI Academy faculty, but who are not assigned as a full-time faculty member.

Advanced Instructor - is a qualified FBI Instructor who is certified and authorized to teach the FBI Instructor Development Course (IDC).

Analysis - is the formal process in which the duties, tasks, knowledge, skills, and abilities are determined for a set of job responsibilities for a particular position of employment. Training needs are the difference between KSAs that are available in the work group and those that will be required in the employment position. The analysis is usually developed in consultation with incumbent employees, supervisors, and others familiar with the job. All aspects of the job, mental, physical, and attitudinal are included in the assessment.

Basic Certified Instructor - is an instructor who has successfully completed the FBI IDC course or the FBI IDC re-fresher course.

Content - information based upon established instructional goals and objectives to include: all main points and supporting content, illustrations, examples, cautions to students, identifies when information meets instructional objectives.

Criteria - the standard by which something is measured. In training it uses the learning objective for the measure of student performance.

Curriculum Materials - all materials required for the presentation of information and the development of skills in formal training.

Design - the phase within the ISD process which includes a description of the training program or course, training setting, the target audience, program duration, learning objectives, testing requirements and description of the general instructional strategies, and methods to be used.

Development - the stage in the ISD process where all training materials, documentation and final evaluation materials are written and produced.

[DRAFT]
FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041870

FBI040770

Evaluation - a process for measuring and assessing student mastery of course objectives; or, for assessing the effectiveness of an overall training program.

Facility - a physical structure used to conduct classroom or practical training or provide support for instruction.

Full-time Instructor - is an FBI employee whose primary role is to provide instruction to New Agent Trainees, National Academy students, Center for Intelligence Training, and/or other Law Enforcement entities.

Grabber - an activity, technique, or ploy to gain attention, motivate, and focus the learner on the topic to learn and content.

Implementation - the phase in the ISD process in which training is delivered as designed, and student mastery of learning objectives is assessed. Training is conducted by instructors who are trained and qualified for the instruction they deliver.

In-service Training - any interim training provided to current FBI employees.

Instruction - the manner in which information is provided to enable learning.

Instructional Goal - is a statement written in broad, general terms that describes what an instructor hopes to accomplish by teaching a lesson.

Instructor Certification - is the confirmation of an instructor's ability to teach.

Instructor Development Program (IDP) - is designed to address training and developmental issues for all FBI Instructors. This training addresses topics such as Adult Learning, Lesson Plan Construction, Methods of Instruction, and the Role of the Instructor. An IDP will also incorporate a number of instructional methodologies such as lectures, discussions, demonstrations, role-plays, laboratories and practical exercises.

Instructor Evaluation - the assessment that is performed by an instructor's supervisor or designee, to determine the instructor's teaching ability, knowledge and skill.

Instructor Notes - documents that are used to identify all actions, activities, and learning points that direct the instructor.

Instructional Objective - a series of statements (one for each learning activity) describing specifically what the instructor expects the student to learn and do as a result of the instruction, to what standard, and under what well-defined conditions.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041871

FBI040771

Instructional Strategies and Methods - activities that are required to teach the material, effect instruction, presentation, practice, and evaluate learning.

Instructional System Design (ISD) - a systematic approach to training (SAT) that includes distinct, yet interacted phases. These phases include: Analysis, Design, Development, Implementation, Evaluation (ADDIE) and Revision.

Instructional Systems Specialist (ISS) - an Instructional Systems Specialist (ISS) administers, supervises, advises on, designs, develops, or provides educational or training guidance regarding formal education or training programs. An ISS is considered the Instructional Systems Development (ISD) SME, and is generally knowledgeable of learning theory and the principles, methods, practices and techniques of one or more specialties of the instructional systems field and responsible for the application of the ISD process to courses and/or lesson plans that they develop, review, or re-write.

Instructional Systems Specialist (ISS) - the role of an ISS is to ensure that each portion of the ISD process is effectively and properly implemented when an instructor is developing lesson plans.

Instructional Technologies and Training Aides - tools used to communicate ideas and support instruction.

Introduction - a statement that identifies the instructor, by providing a personal/professional background to establish credibility.

Learning Objectives - objectives are measurable written statements describing what students will be able to do as a result of training. Objectives normally consist of three parts, a condition under which the behavior will be evaluated, the behavior to be evaluated, and the standard to which the behavior is measured. Learning objectives are based upon the Job Analysis.

Lesson Plan - an instructor's document that outlines instructor and trainee activities, learning objectives, lesson content, and resources necessary for the consistent conduct of training.

Mentor - a senior experienced FBI instructor, or designee who provides guidance and training to new instructors.

National Academy - the FBI National Academy (FBINA) is a professional institution that provides training for state, local, federal and international law enforcement leaders who serve to improve the administration of justice in police departments and other law enforcement agencies.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041872

FBI040772

Needs Assessment - a formal process in which the knowledge, skills, and abilities (KSAs) are determined for a set of job responsibilities for a particular position of employment. It is the difference between the KSAs that are available in the work group and those that will be required in the employment position. The needs assessment is usually developed in consultation with incumbent employees, supervisors, and others familiar with the job. All aspects of the job, mental, physical, and attitudinal are included in the assessment.

Needs Statement - an explanation that established the need to learn the lesson's content, which points out an existing problem or presents a job-related requirement.

New Agents Training - ensures that New Agent Trainees (NATs) receive and successfully complete a 21-week comprehensive training program which provides them with the basic knowledge, skills, and abilities required to safely and effectively serve the citizens of the United States. The New Agent's curriculum is composed of three core areas: Investigative/Tactical, Non-Investigative, and Administrative. The units that provide training for the NAT are the Behavioral Science Unit (BSU), Firearms Training Unit (FTU), Investigative Training Unit (ITU), the Law Enforcement Communication Unit (LECU), Legal and Ethics, the Practical Application Unit (PAU), and the Physical Training Unit (PTU).

Programs - also referred to as courses or groups of training sessions or learning activities conducted for a specific target audience.

Risk Assessment - describes higher risk training operations, such as firearms, defensive tactics, officer survival, etc. Academy management and/or those involved in program development should be keenly aware of the higher risks associated with this type of training and should take appropriate and reasonable measures to mitigate these risks.

Role-player - a contracted actor who is hired by the FBI to assist in the practical application of training by acting out a desired character role.

Short-term Instructor -

Standard - is the portion of an instructional objective that sets the minimum level of acceptable performance. It allows students to be measured in terms of pass/fail and measures the effectiveness of instruction.

Subject Matter Expert (SME) - is an employee with the special skill or knowledge representing mastery of a particular subject.

Summary - is the area of the lesson plan which serves to reinforce the ideas and concepts that are presented in a lesson, offers feedback, and provides the psychological closure of the lesson.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041873

FBI040773

Systematic Approach to Training (SAT) - is a systematic method for establishing and maintaining training programs. Following an SAT ensures that essential knowledge and skills are identified, taught, and evaluated for successful job performance.

Tactical Emergency Vehicle Operation Center (TEVOC) – training that is designed to teach safe, efficient driving techniques to FBI and DEA personnel, other government and military personnel, as well as Legat personnel.

Task - is a defined unit of work having an identifiable beginning and end that is a measurable component of the duties and responsibilities of a specific job.

Task Analysis - is a complete and orderly step-by-step process which enables a task to be performed from beginning to end. Task analysis should include the description of the task; conditions under which the task is performed and the standards that must be met to meet a level of acceptable performance.

Task Step - is a single action performed as a set of actions that are necessary to complete a job.

Thesis Statement - is a specific statement that describes the goals of the course clearly stating the purpose of the lesson, where the student currently is and where the student is going. This can be a reiteration of the instructional goal stated in the Statement of Goals and Objectives.

[DRAFT]
FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041874

FBI040774

3 Instructional Certification

3.1 FBI personnel who are selected to provide instruction to New Agent Trainees, National Academy students, Center of Intelligence Training, and other Law Enforcement entities; must enroll in, attend, and successfully complete the FBI Instructor Development Course (IDC). See EC dated 6/4/2007, [REDACTED] DRAFT.

b7E

3.2 Training instructors who teach high-risk areas such as firearms, intermediate weapons, first aid, physical control techniques and Tactical Emergency Vehicle Operation Center (TEVOC) must also complete and maintain certification and/or continued education for each specialized area in which they provide instruction.

3.2.1 With regard to instructors, any information regarding training, conferences or research initiatives, should be captured on the *Continuing Education form (FD-932)* or within a unit training database and maintained in the instructors personnel file.

3.3 All instructors will need to be re-certified every 5 years, if they intend to continue to provide instruction. Maintaining instructor certification will ensure that FBI instructors have the training, skills and ability to meet and address training challenges with confidence and an improved level of expertise.

3.4 FBI Instructor development courses will be taught in a classroom environment, and a variety of techniques and practical exercises will be incorporated into the process.

3.5 If instructors from other entities are providing training to New Agent Trainees and/or National Academy students, or the Center for Intelligence Training, their qualifications must be verified and approved TD Section and/or Unit Chiefs prior to their arrival.

4 Training Development, Responsibilities and Requirements

Codes of conduct, rules and requirements, violations and consequences of prohibited conduct or activities, identification of inappropriate behavior for instructors, safety rules and regulations will be specifically addressed for instructors, as part of their orientation for instructor training.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

4.1 Instructor Requirements

4.1.1 The FBI Academy requires that its instructors, with the exception of those teaching technical skills, have at a minimum, a Baccalaureate degree...(KSA and training required to ensure staff maintain the position qualification requirements.) ????

4.1.2 The FBI Academy requires that instructors who provide instruction for the National Academy must have X amount of years of experience in the area in which he/she will be providing instruction. Ask UC

b6
b7c

4.1.3 The University of Virginia (UVA) is accredited by the Commission on Colleges of the Southern Association of Colleges and Schools (CCSACS). Based on the standards set forth by CCSACS, UVA requires that instructors who teach NA students have a master's or doctorate degree in the teaching discipline, or a master's degree with a concentration (a minimum of 18 graduate semester hours) in the teaching discipline.

4.1.4 The FBI Academy requires full-time instructors to have, at a minimum, a Baccalaureate degree and/or the knowledge, skills and abilities to perform instructional tasks effectively.

4.1.5 The FBI Academy requires adjunct or part-time instructors to have, at a minimum a Baccalaureate degree and/or the knowledge, skills and abilities to perform instructional tasks effectively.

4.1.6 Contracted instructors and some guest or adjunct instructors may be exempt from having to receive certification via the FBI IDC course. This decision may be determined by the applicable SC, UC or his/her designee.

4.1.7 Contract instructors must agree to provide the FBI Academy (???) with documentation of their expertise as it applies to the training program and must agree to incorporate the required learning objectives of the course, into their lesson plan.

4.2 Instructor Development and Responsibilities

It is imperative that all instructors at the FBI Academy are certified, maintain their certification, and maintain currency and proficiency in the subject matter in which they provide instruction, and collaborate with Instruction Systems Specialists (ISSs) when developing lesson plans that are required for instruction. To further ensure that the FBI Academy meets the standards required to maintain accreditation by FLETA, ISSs must be available to assist Instructors with the proper application the ISD process to develop technically and systematically effective lesson plans.

[DRAFT]
FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

4.2.1 Section Chiefs will be responsible for:

- Ensuring that instructor development and training is made available within all Instructional units of the FBI Academy.
- Maintaining and implementing the divisional training initiatives for instructors.
- Ensuring that supervision and guidance is available to all instructors within their section.
- Ensuring that all adjunct, contract, and/or guest instructors abide by policies and guidelines set forth by the FBI Academy.

4.2.2 Unit Chiefs will be responsible for:

- Ensuring that instructor development and training is made available to instructors within his/her unit.
- Ensuring that supervision and guidance is available to all instructors within their unit.
- Ensuring that Instruction is listed as a critical element on Performance Appraisal for those employees who are certified instructors.
- Informing the TD FLETA OA of when new instructors have successfully completed training and/or re-certification, and have been certified to perform instruction without supervision.

4.2.3 Supervisors will be responsible for:

- Reviewing and discussing the requirements of the FBI Academy's training plan with each new instructor.
- Ensuring successful completion of mandatory instructional staff training courses, to include refresher courses when applicable; and capturing this information via the *Continuing Education form (FD-932)*, or computer database.
- Assigning a certified instructor or training staff member to new instructors to mentor and review training requirements as needed.
- Conducting instructor evaluations on the *Performance Appraisal (PAR) form (FD-727.2)* bi-annually, and maintaining copies of the evaluations in the instructors file.
- Maintaining signed and dated copies of all instructor training certificates and training records.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041877

FBI040777

4.2.4 Mentors and/or Training Officers will be responsible for:

- Reviewing and discussing the requirements of the FBI Academy's training plan with each newly assigned instructor.
- Assisting new instructors with the preparation of lesson plans.
- Reviewing lesson plans of new instructors to ensure accuracy and completeness.
- Monitoring and acting as an advisor in the classroom setting once the new instructor is assigned to instruct a course.
- Providing new instructors with relevant and applicable feedback.

4.2.5 Instructors will be responsible for:

- Providing accurate, detailed and current information when delivering instruction to New Agent Trainees, National Academy attendees, Center for Intelligence Training attendees, and other Law Enforcement entities as applicable.
- Applying the five phases of the Instructor Systems Design (ISD) model which include: Assessment/Analysis, Design, Development, Implementation, and Evaluation when constructing lesson plans.
- Reviewing and revising the information contained in each lesson plan as required, and documenting that the review and/or revision process has been completed.
- Providing role-players with information in preparation for scenarios that will be acted out during practical application training, when applicable.
- Maintaining their proficiency and providing current information on subject matter.
- Documenting all phases of the lesson plan development and implementation.
- Maintaining student records in accordance with the policies detailed in dated December 6, 2006.

b7E

4.2.6 Instructional Systems Specialists will be responsible for:

- Assisting Instructors with the preparation of courses and lesson plans that will be developed, reviewed and/or re-written.
- Administering and applying the systematic methods of the ISD process to the preparation of lesson plans.
- Providing educational and/or training guidance for formal education and training programs provided by the FBI Academy.

4.3 Providing Instructor Development Training

Instructors must be provided with written information and/or an orientation that includes but may not be limited to the following:

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041878

FBI040778

- The mission and vision of the FBI Academy.
- Code of conduct rules and requirements.
- Understanding of violations and consequences of prohibited conduct or activities.
- Identification of inappropriate behavior for instructors, students and their visitors.
- Organizational charts.
- FBI Academy safety rules and regulations, fire and emergency procedures as set forth in MAOP, MIOG, the FBI TD Safety Manual, and any unit specific policies and procedures.

All instructors must complete required periodic training on EEO, Sexual Harassment and other mandated training. This training must be documented and all applicable training documentation must be maintained in his/her file.

4.3.1 Newly appointed instructors are required to receive training by attending the 40 hour block of instruction provided in the FBI Instructor Development Course (IDC), and must successfully complete the course. The FBI IDC will address areas of instruction which will include, but are not limited to:

- The Basics of Designing Instruction.
- The Fundamentals of the Instructional Design System (ISD).
- Learning Objective Development.
- Lesson Plan Development.
- The Fundamentals of Adult Learning.
- Assessing Training Needs.
- Task Analysis.
- Evaluating Instruction for Effectiveness.
- Testing and Evaluation Techniques.
- Creating Tests and Test Instruments.
- The Basics of Instruction.
- Leadership, Ethics and Legal Responsibility

4.3.2 If an instructor has been certified via methods other than the FBI IDC, instructs occasionally, or has not maintained his/her certification, he/she will be required to attend the FBI IDC refresher course, and must successfully complete the IDC refresher course.

4.3.3 Review and revise the information contained in each lesson plan as required, and document that the review and/or revision process has been completed.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

5 Criteria for Successful Completion of Instructor Training

Those who attend the FBI Instructor Development course will be evaluated on the following:

- Instructional Goals and Objectives.
- Interactive Presentation (5 minute presentation).
- Final Presentation (20 minute presentation).
- Preparation of a Student Lesson Plan

5.1 The minimum passing grade of 80% is required for successful completion of the FBI IDC course and if applicable, the FBI IDC refresher course.

5.2 Upon successful completion of the FBI IDC training, instructors will be required to:

- Use the accepted Lesson plan format (see [redacted] dated 4/17/2007) and all related forms when preparing instructional lesson plans. For further information please refer IDC manual.
- Collaborate with ISSs when developing lesson plans to ensure that the five phases of the Instructor Systems Design (ISD) model which include: Assessment/Analysis, Design, Development, Implementation, and Evaluation are used and applied correctly.
- Maintain current information on subject matter and make revisions to instructional content when required as needed.
- Document all phases of the construction, task analysis, and review of each lesson plan.
- Review and revise the information contained in each lesson plan as required, and document that the review and/or revision process has been completed.

b7E

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041880

FBI040780

6 Instructor Mentoring, Evaluation and Remediation

6.1 Once a new instructor has successfully completed the IDC, he/she will work in a Team-Teach environment with his/her assigned mentor for at least 2-3 months prior to being able to provide instruction solely on his/her own.

6.2 The mentor of the new instructor will be required to provide the new instructor with constructive feedback and support as deemed necessary.

6.3 If required, an instructor may be recommended for remediation and/or re-evaluation. The steps to address instructor remediation and re-evaluation will be addressed via guidance set forth in the IDC Re-fresher course.

7 Recordkeeping Requirements

7.1 FBI Academy policy is set forth in this Accreditation Manual, as well as in other internal and external documents. Policy statements and any revisions to this policy and guidelines manual will be approved by the AD, the Accreditation Manager and, if applicable, Section or Unit Chiefs, prior to issuance.

7.2 FBI Academy program or unit specific instructional lesson plans will be located in each program or unit, respectively. Prior to implementation, lesson plans will be reviewed by the applicable Section Chiefs (SCs) and Unit Chiefs (UCs) of the FBI Academy, the TD FLETA OA, Instructional Systems Specialists (ISSs) and the Instructor. Any revisions must be approved by the AD, and the TD FLETA OA.

7.3 All FBI Academy records will be legible and readily retrievable from storage in appropriate FBI facilities. Retention times for records will be determined by Records Management Division policy and/or FLETA requirements.

7.4 Access to FBI Academy files will be controlled according to FBI policies.

7.5 Electronic records located in the Automated Case Support (ACS) system and FBI Trilogy system will be maintained by the Information Technology Operations Division (ITOD). Access to these records will be controlled. Each unit should have procedures for backing up records that are not located on the FBI Trilogy systems.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041881

FBI040781

8 Document Control

Documents that specify training and/or instructional requirements or prescribe quality-affecting activities must be controlled to ensure that they are adequate, that they have been approved for use and that only the current version of the documents/lesson plans are in use. Prior to their implementation it is imperative that instructional materials are review by approved staff members, TD FLETA OA, UCs, and when required, SCs.

Copies of all instructional documents/lesson plans, guidelines and/or manuals produced within the FBI Academy for instructional and/or accreditation purposes must be forwarded to the TD FLETA OA.

8.1 Lesson Plan Approval and Issuance

When applicable, all changes to curriculum must first be reviewed and approved by the New Agents Training Program Curriculum Committee (NATPCC) and other authorized personnel.

8.1.1 Prior to implementation, all FBI Academy training system lesson plans and the Instructional System Design of the lesson plans will be thoroughly reviewed, approved for release by authorized personnel. Upon approval, the lesson plan(s) will be made available for use by approved employees.

8.1.2 Current versions of instructional documents and lesson plans must be readily available.

8.1.3 FBI Academy instructional documents and/or lesson plans must be uniquely identified. This identification includes the document title, date of issue, revision number, and page numbering including total number of pages. The approving and issuing authorities will also be identified in the document.

8.2 Revisions to Instructional Material

8.2.1 Revisions to FBI Academy instructional documents and/or lesson plans will be subject to the same review, approval, documentation and issuance requirements as the original document. Changes to documents will be described in the revision history portion of the document. Additionally, appropriate personnel must have access to any information necessary to conduct the review and approve the revision.

8.2.2 The FBI Academy's accreditation system will not permit the amendment of documents by hand for internally prepared documents.

[DRAFT]
FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041882

FBI040782

8.3 Responsibilities

The FBI Academy is an elite law enforcement agency. Providing training to new agent trainees and other law enforcement personnel is an integral part of the FBI Academy. As part of the approval process, any guidelines, policy documents and/or manuals that have any bearing on the accreditation process must be submitted to the TD FLETA OA for review.

In order for superior lesson plans and training to be developed it is vital for all components associated with curriculum development to be applied effectively. The responsibilities for those involved in the process are as follows:

8.3.1 The Instructor will:

- Prepare the lesson plan and/or other instructional documents in the proper format.
- Collaborate with an ISS to ensure that the ISD process is properly applied in the process of creating the lesson plan.
- Write the lesson plan with a level of detail commensurate with the complexity of the activity and the background of the expected user.
- Submit the lesson plan and the *TD FLETA OA Document Review Form (2-XXXX)* for technical and quality assurance review.
- Address and/or resolve comments from the reviewers.
- Provide the lesson plan and the completed *TD FLETA OA Document Review Form (2-XXXX)* to the TD FLETA OA.

8.3.2 The Instructional Systems Specialist(s) will:

- Thoroughly review lesson plan(s) and/or other instructional documents for technical accuracy, sufficiency, and clarity of presentation.
- Work with instructors/SMEs to ensure that each step of the ISD process is properly addressed, documented and applied to the development of all lesson plans and other instructional documents as required.
- Document the technical review on the *TD FLETA OA Document Review Form (2-XXXX)*.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041883

FBI040783

8.3.3 The TD-FLETA OA Reviewer(s) will:

- Check the document for inclusion of appropriate quality requirements, quality sufficiency, and adherence to all division policies and practices.
- Document the quality assurance review on the *TD FLETA OA Document Review Form (2-XXXX)*.
- Ensure that the technical and quality assurance reviews have been completed and documented for division policies and practices.
- Ensure that the technical and quality assurance reviews have been completed and documented for unit quality manuals.
- Ensure that the documents are suitable to be issued.
- Ensure that all division controlled policies and practices are reviewed annually.
- Make a copy of the *TD FLETA OA Document Review Form (2-XXXX)* to return to the preparer.

8.3.4 The Unit Chief will:

- Ensure that the technical and TD FLETA OA reviews have been completed and documented for policy manuals/documented and standard operating procedures.
- Ensure that training and instructional documents have been reviewed.
- Ensure that the documents are suitable to be issued.
- Ensure that all unit controlled documents are reviewed annually.

8.3.5 The Issuer or the person in charge of revising the document(s) will:

- Obtain appropriate approvals to issue the document.
- Distribute the document to appropriate personnel.
- Retain distribution records.
- Collect and maintain a file of superseded documents.
- Distribute subsequent revisions and provide the TD FLETA OA with a copy of the revised document.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041884

FBI040784

8.4 Format

Guidelines, policy documents and manuals that have any bearing on the accreditation process should be formatted in accordance with the requirements set forth by the Corporate Policy Office (CPO) and when applicable, the FBI Instructor Development Course (IDC).

8.4.1 Each page of a lesson plan should have a right justified header. The header should include at least the following information, in this order:

- Title of the Block of Instruction
- Document Title or name of the Lesson Plan
- Revision Number
- Effective Issue Date
- Pagination (Page _ of _)

8.4.2 Each page of a lesson plan should have a justified footer in the center. The footer will indicate the status of the document as being controlled, uncontrolled or a draft.

8.4.3 The revision history will be comprised of three columns. The first column will consist of the revision number, the second will be the issue date of that revision and the third will contain a brief statement detailing the changes were made to the document.

8.4.4 The signature block will be located after the revision history of the lesson plan/course map, and will be comprised of five sections. The first section will contain the approval signature line and date for the Section Chief of the issuing unit. The second section will contain the approval signature line and date for the Unit Chief. The third section will contain the TD FLTEA OA approval signature and date. The fourth section will contain the issuer's signature and date. Lastly, the fifth section will contain the approval signature and date for the Instructional Systems Specialist (ISS).

8.4.5 The TD FLETA OA will review proposed revisions to the FBI Academy quality system to ensure that the integrity of the system is maintained when changes are implemented.

8.4.6 Instructional documents and/or lesson plans will be annually reviewed by Instructors/SMEs and ISSs as required and revised as necessary to comply with applicable requirements set forth by FLETA.

8.4.7 Invalid or obsolete documents must be promptly removed and archived documents will be marked as such to preclude their use.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041885

FBI040785

9 Training Requested or Provided by Outside Entities

Memorandums of Understanding (MOUs), contracts or any other form of written agreement should be completed to establish responsibility and accountability for the training being conducted. Written agreements must be approved by the OGC, the TD Assistant Director or designee prior to entering into an official agreement. Documentation of training that has been requested and/or provided by outside entities must be documented.

9.1 Any documentation relating to training that has been requested and/or provided by outside entities must be maintained by the unit/program in which the request was made.

9.2 A copy of the documents must be forwarded to the TD FLETA OA.

10 Use of Licensed and Copyrighted Material

In accordance with U.S. copyright laws, permission must be obtained from the originating individual or organization prior to the use of most licensed and/or copyrighted material. (see *MAOP Part 2 Section 11(4) Miscellaneous Regulations and Title 17, United States Code*).

10.1 Licensed and copyrighted material includes both printed and electronic forms of information.

10.2 Documentation regarding the authorized use of licensed and copyrighted material must be maintained by the requesting unit/program, when applicable.

11 Safety Considerations and Risk Assessments

There is an inherent risk of injury with some types of law enforcement training. As a result, the safety of all students and staff at the FBI Academy is vital. Managers and instructors of the FBI must ensure that training is conducted in an environment which is conducive to the safety and well-being of all students and staff. Training will be conducted in facilities that are in compliance with Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA) regulations and

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041886

FBI040786

standards, and the codes and requirements set forth by the National Fire Protection Agency (NFPA).

11.1 FBI management and instructors must ensure that the appropriate equipment and facilities are made available for all training initiatives.

11.2 Equipment/facility requirements must be provided in the lesson plan that is provided for each block of instruction.

11.3 Training Risk Assessment must be conducted to identify potentially dangerous types of training. Management and instructors must ensure that all mitigating factors that are outlined in a risk assessment are complied with.

11.4 Prior to their involvement in any practical exercises/examinations or firearms training, a safety briefing will be administered to all students, role-players and other personnel who may participate.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041887

FBI040787

Appendix A: Acronyms

AD	Assistant Director
ADDIE-R	Analysis, Design, Development, Implementation, Evaluation and Revision
BSU	Behavioral Science Unit
CIT	Center for Intelligence Training
DAD	Deputy Assistant Director
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
EAP	Employee Assistance Program
EC	Electronic Communication
EEO	Equal Employment Opportunity
FLETA	Federal Law Enforcement Training Accreditation
FTU	Firearms Training Unit
IDC	Instructor Development Course
IDP	Instructor Development Program
ISD	Instructional Systems Design
ISS	Instructional Systems Specialist
ITOD	Information Technology Operations Division
ITU	Investigative Training Unit
KSA	Knowledge, Skills and Ability
LECU	Law Enforcement Communications Unit
MAOP	Manual of Administrative Operations and Procedures
MIOG	Manual of Investigative Operations and Guidelines
NA	National Academy
NATPCC	New Agents Training Program Curriculum Committee
NATP	New Agent Training Program
NATU	New Agent Training Unit

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041888

FBI040788

OA	Office of Accreditation
PAU	Practical Applications Unit
PTU	Physical Training Unit
SC	Section Chief
SME	Subject Matter Expert
TD	Training Division
TEVOC	Tactical Emergency Vehicle Operation Center

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041889

FBI040789

Appendix B: Sources of Additional Information

Commission on Colleges of the Southern Association of Colleges and Schools (CCSACS), Principles of Accreditation, December 2001

Electronic Communication (EC) [REDACTED] Title: New Agent Training Program Curriculum Committee Meeting; Minutes and Recommendations, dated April 17, 2007.

Electronic Communication *DRAFT* (EC) [REDACTED] Serial ???; Title: Recognition of the Current Instructor Development Course and an Approved Requirement for Instructors, dated June 4, 2007.

Electronic Communication (EC) [REDACTED] Title: Establishment of the Curriculum Audit Process and Policy NATCC/NAATPS, dated June 22, 2007.

Federal Bureau of Investigation (FBI) Instructor Development Program - Student Learning Guide (2006). 2nd Edition.

Federal Bureau of Investigation (FBI) Security Bulletin

Federal Law Enforcement Training Accreditation (FLETA) Standards Guide, December 2005

Manual of Administrative Operations and Procedures (MAOP), Federal Bureau of Investigation (FBI), March 12, 2007

Manual of Investigative Operations and Guidelines (MIOG), Federal Bureau of Investigation (FBI), April 17, 2007

Memorandum to All Employees 9-2001 Re: Continuing Development and Training of FBI Employees, Federal Bureau of Investigation, August 7, 2001.

U.S. National Archives & Records Administration Executive Order 12958-Classified National Security Information, dated January 6, 2004.

United States Code, Title 17

United States Code, Title 28, Section 533.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041890

FBI040790

Appendix C: Forms

TD-FLETA OA Document Review Form

Preparation

The following document has been prepared and is being submitting for review.

Document Title: (print)			Revision No.:
Preparer: (print)	Initials:	Unit:	Date:

Technical Review

I have reviewed the above document for technical accuracy and clarity of presentation and judge it to be acceptable for issuance.

Technical Reviewer (print):	Initials:	Unit:	Date:

TD FLETA OA Review

I have reviewed the above described document for conformance to the applicable policies, practices and procedures of the quality system and judge it to be approved for use.

TD FLETA OA Reviewer (print):	Initials:	Unit:	Date:

Preparer(s):

Will complete the preparation section of the document review form. Submit this form, along with the final version of the document, to the technical reviewers. When the technical review is complete submit the document and review form to TD FLETA OA for review.

Technical Reviewer(s):

Will review the document for technical accuracy and clarity of presentation. If the document is acceptable, complete the technical review section of the form and return the document and review form to the preparer. If the document is not acceptable, return it to the preparer for corrections.

TD FLETA OA Reviewer(s):

Will verify that the final version of the document conforms to applicable accreditation policies, practices and procedures. Complete the TD FLETA OA review section of the form. Make a copy of the completed form and return the copy and the document to the preparer. TD FLETA OA will maintain the originals copies of document review forms.

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041891

FBI040791

Edition# Issue Date**History**

1 11/01/07 Intro. of Instructor Development Policies & Guidelines

Approval and Issuance

Training Division

Assistant Director: _____

Brian D. Lamkin

Date: _____

RMO Section Chief: _____

Charles P. Taylor

Date: _____

SPPU Unit Chief: _____

Date: _____

ITU Unit Chief: _____

Date: _____

TD FLETA OA

Program Manager: _____

Date: _____

b6
b7C

[DRAFT]

FOR FBI INTERNAL USE ONLY – DO NOT DISSEMINATE
SENSITIVE

ACLURM041892

FBI040792

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-17-2011 BY 65179 DMH/STW

National Counterintelligence (CI) Training Standards and Guidelines

2007

UNCLASSIFIED
ACLURM041893

FBI040793

UNCLASSIFIED

Table of Contents

Section A Guidelines	Introduction: A Context for National CI Training Standards and 1. Terminology Used and Rationale a. Use of term standards and guidelines b. Rationale for use of terms 2. Scope of Application and Need for CI Training, Standards, Guidelines a. Scope of Application b. Need for Standards and Guidelines 3. Development Process for CI Standards and Guidelines a. Participants and Process b. Policy and Resource Documents
Section B	Implementation and Maintenance of CI Standards and Guidelines 1. Plan for Promulgating Proposed Standards and Guidelines 2. Plan for Maintaining Currency of Standards and Guidelines
Section C	CI Standards and Guidelines 1. Level I – Basic – CI Generalist 2. Level II – Journeyman – CI Generalist 3. Level II – CI Technical Function Areas a. CI Operator and Collector b. CI Investigator c. CI Analyst
Section D	References
Section E	Appendices

UNCLASSIFIED

Section A:
Introduction: A Context for National CI Training Standards and Guidelines

1. Terminology Used and Rationale for Standards and Guidelines

“The terms *standards* and *guidelines* are often used interchangeably or inconsistently in the context of education and training. In an effort to achieve more consistency and appropriate use of these terms, therefore, the following paragraphs provide the definition and clarification of the different contexts in which they are typically used in national education communities.” (“Developing and Evaluating Standards and Guidelines Related to Education and Training in Psychology: Context, Procedures, Criteria, and Format,” American Psychological Association (APA), February 20, 2004)

(a) Use of Terms

Standards

Standards are defined in this document as any criteria or specification for conduct, performance, or products in counterintelligence (CI). This definition satisfies the conditions expected of a standard as defined by national education communities – i.e. benchmarks established for use as a rule or basis of comparison in measuring or judging capacity, quantity, content, extent, value, quality, etc. (as quoted by APA from Kendall, 2001; and National Center for Education Statistics, 2001). National CI Standards are considered mandatory and may be accompanied by an enforcement mechanism produced by the Office of National Counterintelligence (ONCIX) and the Office of the National Director of Intelligence (ODNI).

Guidelines

Guidelines are defined in this document as pronouncement, statements, or declarations that suggest or recommend specific behaviors, endeavors, or conduct for CI personnel. Guidelines are an advisory set of procedures related to curriculum development or assessment; as an interpretive commentary or instruction on education policy or standards; as a set of guiding principles about teaching and learning, or program development; or suggested goals and objective of learning. Guidelines are intended to be neither exhaustive nor mandatory, but are intended as suggestions or recommendations for the CI Community.

(b) Rationale for Use of the Terms

UNCLASSIFIED

In the national context of postsecondary levels of training, including preparation for professions, the terms *standards* and *guidelines* are both used, sometimes in combination. In this context, the term *standard* is used to refer to a minimal (threshold) requirement for training. Standards are mandatory, and may be accompanied by guidelines that provide interpretive clarification on how they may be met or how their achievement may be assessed. The purpose for promulgating and implementing these standards and guidelines is to improve the quality of instruction, learning, and performance within the CI discipline.

2. Scope of Application and Need for National CI Training Standards and Guidelines

(a) Scope of Application

National CI Standards and Guidelines apply to all U.S. government agencies, organizations, and private training activities that provide CI training to Federal personnel or oversee personnel who perform jobs within the CI discipline. This document encompasses minimum training standards for all CI personnel at the CI generalist level I (Basic) through the CI level II (Journeyman). Level II includes those personnel performing specific technical functions of CI operations, collection, investigations, and analysis. All personnel subject to these standards will possess at least a high school diploma or GED.

These CI training standards will be implemented across all U.S. government agencies and organizations that contain a CI mission. In the case of privately contracted CI training, the contracting government agency will be responsible for including required CI training standards in Statements of Work (SOW) if the contracted training is expected to meet these standards and satisfy CI personnel training requirements.

This CI training standards document is designed to apply to all U.S. personnel filling a position in the CI discipline. The CI Generalist, Level I (Basic) outlines the mandatory minimum training required for all CI personnel. The Level II standards for specific CI technical functions provide a mandatory minimum requirement for CI personnel in specific area(s) of assignment – analysis, operations, investigations, collection. However, U.S. government agencies/organizations may add additional CI training standards to those presented in this document for the purpose of addressing their unique CI missions.

U.S. government agencies and organizations will use this standards and guidelines document to inform CI curriculum development, professional development plans, and career paths. The mandatory set of standards will be established in authority by the National CI Policy Board and an Intelligence Community Policy Guidance (ICPG) made part of the CI Intelligence Community Directive (ICD). These standards will be enforced via peer reviews of training curricula and budget-based CI program reviews.

(b) Need for Standards

UNCLASSIFIED

The need for national CI training standards and guidelines have been recognized at the national level at least since PDD-75 and the CI Enhancement Act of 2002 [look up specific references]. Most recently, the WMD Commission Report (2005) recommended that the Office of National Counterintelligence (ONCIX) develop common training standards for the CI Community to professionalize the CI workforce. The National CI Strategy (2007), Enterprise Objective (E.O.) 1 and 2 require that common CI training standards be developed for the CI community to professionalize the CI cadre [look up specific references for quotes]

Without national CI training standards and guidelines, the quality and extent of CI training will continue to be ad hoc and inconsistent across the Federal government. A common baseline of training for the CI generalist at the basic level and the CI technical functions at the journeyman level is required to professionalizing the CI discipline. Standards for a common basic level of training is fundamental to facilitating collaborative activities and efforts across the U.S. government agencies as required by the Director of National Intelligence (DNI). In addition, a standard level of training is required for preparing professional development plans and career tracks for the CI workforce. Until CI personnel have mandatory common training standards at the basic and journeyman levels that are subject to oversight, one of the elements that determine an activity as a profession will be lacking [see definition of profession in Vol 1]

3. Development Process for National CI Training Standards and Guidelines

(a.) Participants and Process

The National CI Training Standards and Guidelines are derived from the CI Competency study described in Volumes 1 and 2 [reference full titles]. As noted in both volumes, the competency results of the study and the volumes as well, were coordinated through the CI Community before publication in 2006 and 2007, respectively.

..... Expand on methodology for deriving training standards from the competencies and KSAs.....

The training standards published in this document were coordinated throughout the CI Community in a similar manner to that used in the Competency Study.

UNCLASSIFIED

UNCLASSIFIED

Laws, Policies and Jurisdictions

Standard G1 The student will understand the US statutory and regulatory guidance that governs activities of the counterintelligence (CI) discipline.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will understand US laws and policies that govern intelligence and CI activities, to include the US Constitution, FISA, and use of the Freedom of Information and Privacy Acts, and to understand applicable Executive Orders, Federal laws and agency regulations and policies.

Laws

- G1.1 Locate, read and comprehend applicable US laws and individual constitutional protections.
- G1.2 Apply proper oral legal rights advisements and warnings.
- G1.3 Collect, document, preserve, store and transport evidence while maintaining chain of custody.
- G1.4 Demonstrate knowledge of standard evidence protocols of other government agencies to preserve prosecutorial integrity.

Policies

- G1.5 Demonstrate knowledge of Attorney General Guidelines in conducting CI activities.
- G1.6 Understand the process to properly classify documents in accordance with applicable classification guides and policies.
- G1.7 Understand US Foreign Policy as it relates to CI activities against specific countries.
- G1.8 Display knowledge of the national intelligence and counterintelligence strategies for the community and individual organizations.
- G1.9 Understand the Intelligence Oversight policies and requirements.
- G1.10 Understand and comply with all organizational CI policies and procedures.
- G1.11 Demonstrate proficiency in proper inter and intra-agency requirements for reporting CI activities.
- G1.12 Understand what technologies are admissibility in court.
- G1.13 Use intelligence, investigative and tradecraft terms that are clear and based on common definitions.
- G1.14 Exploit the best operational methodologies available to an individual organization against priority targets.

Jurisdictions

- G1.15 Demonstrate knowledge of assigned agency mission and objectives.
- G1.16 Understand jurisdictional differences between CI and other intelligence disciplines.

UNCLASSIFIED

- G1.17 Evaluate the significance of key historical CI events and cases in the development of the CI discipline as an aid to operational and investigative decision-making.

Standard G1 maps to the following competencies:

- Reading Comprehension
- Oral Communication
- Laws, Policies, Procedures & Jurisdiction
- Critical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Risk Management

UNCLASSIFIED

Standard G2 maps to the following competencies:

- Reading Comprehension
- Oral Communication
- Analytical Thinking
- Critical Thinking
- Decision Making
- Evaluation and Critique
- Risk Management
- Customer Awareness
- Interpersonal Skills

UNCLASSIFIED

Data Assimilation and Use

Standard G3 The student will show an appreciation for the tools and techniques used in gathering information to use in CI analysis.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will be familiar with the various sources and techniques used to gather information for analysis. They will understand the importance of validating the reliability of this information and how to structure the data for analysis. Students will have a familiarization of analytical tradecraft and how it enhances analytical products and supports activities performed in other functions of the CI discipline.

Gather

- G3.1 Correlate data from different sources and cluster data according to logical relationships.
- G3.2 Use data-mining for identifying data from different databases and sorting through data to identify patterns and establish relationships.
- G3.3 Extract important information from volumes of data to ascertain associations and significant details.
- G3.4 Recognize behavior patterns and trends, and interpret as significant indicators.
- G3.5 Recognize and analyze anomalies, trouble spots, and unresolved issues.
- G3.6 Know where and how to find data and sources of information relevant to specific projects.
- G3.7 Understand the importance of using open source material.

Validate

- G3.8 Determine the reliability of gathered information (etc.).
- G3.9 Validate information and research data, and caveat accordingly.

b7E

Structure

- G3.10 Prioritize data and present data/information in a useful format.
- G3.11 Use sifting, sorting, and categorizing to organize related information.

Manipulate

- G3.12 Choose and implement appropriate analytical methods, approaches, and tools (e.g. link analysis).
- G3.13 Build a "story board" (i-notebook) for use in isolating key information.
- G3.14 Organize the development of data through manipulation.
- G3.15 Build and use matrices to depict, organize, and compare the main elements of the data.
- G3.16 Develop and use timelines to create visualization of the sequence and relationships between important facts and events.

Standard G3 maps to the following competencies:

- Reading Comprehension
- Written Communication
- Oral Communication
- Creative Thinking
- Analytical Thinking
- Critical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Planning
- Evaluation and Critique
- Automated Data Systems
- Risk Management
- Customer Awareness

Documenting Information and Communicating Intelligence

Standard G4 The student will prepare products that have a clear focus, unbiased detail, and coherent organization.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will cull important information from a variety of sources. They will prepare and deliver oral and written communication using correct English grammar, punctuation, and spelling that is appropriate for the intended audience.

Document

- G4.1 Create comprehensive notes by using techniques such as lists, paraphrasing and/or summarizing discussions, or evaluating information and charts/graphs, etc.
- G4.2 Create outlines to organize information and develop the content of the work product.
- G4.3 Use an established, standardized system to document CI activities according to customer needs.
- G4.4 Use an established system of record-keeping that clearly provides the source of gathered information.

Prepare

- G4.5 Develop and advocate a position using example, facts, and statistics derived from research work and experience.
- G4.6 Produce clear and concise oral presentations.
- G4.7 Express written ideas in an effective, clear, accurate, and succinct manner utilizing correct grammar, spelling, and rules of classification.
- G4.8 Clarify a position, prepare an argument, and organize a persuasive written report.
- G4.9 Demonstrate knowledge of intelligence reporting formats.
- G4.10 Demonstrate writing flexibility by adjusting style, format, and content of the communication to the intended audience.
- G4.11 Understand the importance of preparing IIRs for communicating with the U.S. Intelligence Community.

Produce

- G4.12 Compose detailed written documents from key CI information.
- G4.13 Produce objective reports supported by reliable evidence.
- G4.14 Knowledge of standard styles and format used in intelligence publications.

UNCLASSIFIED

Convey

- G4.15 Understand interagency roles, responsibilities, and missions when communicating across the US Intelligence Community.
- G4.16 Market the significance of CI capabilities, products, and services to the US Intelligence and Policymaking Communities.
- G4.17 Conduct presentations and briefings on activities and products.
- G4.18 Understand the procedures for sharing information throughout the US Intelligence Community.
- G4.19 Use various communication systems within the US Intelligence Community (i.e.).
- G4.20 Communicate intelligence while appropriately protecting source information.

b7E

Standard G4 maps to the following competencies:

- Reading Comprehension
- Written Communication
- Oral Communication
- Creative Thinking
- Analytical Thinking
- Critical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Evaluation and Critique
- Laws, Policies, Procedures and Jurisdictions
- Concept Facilitation/Influencing/Negotiating
- Automated Data Systems
- Risk Management
- Customer Awareness
- Interpersonal Skills

UNCLASSIFIED

Collaboration

Standard G5 The student will demonstrate the ability to work in a collaborative and cooperative manner, functionally within his/her own organization and externally with other federal law enforcement and intelligence agencies.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will understand the value of collaboration and how working with other agencies of the CI Community and other disciplines of the IC can enhance overall CI capabilities and outcomes.

- G5.1 Establish processes that ensure an understanding of the end-user information needs and circumstances.
- G5.2 Understand the mission, equities and requirements of customers of CI activities.
- G5.3 Demonstrate familiarity and understanding of collection and offensive CI operations.
- G5.4 Demonstrate an understanding of the capabilities of other IC organizations and how they can support CI activities.
- G5.5 Forge positive and constructive relationships at appropriate levels within domestic and foreign law enforcement and intelligence organizations.
- G5.6 Demonstrate collection/reporting and investigative activity that separates content from sensitive sources and methods while providing other organizations with sufficient context, detail and background to meet their mission needs.
- G5.7 Coordinate plans based on purposeful, open and consistent information exchanges.
- G5.8 Negotiate CI plans and activities with other agencies giving appropriate weight to customer needs.
- G5.9 Use instituted arbitration and adjudication processes to resolve disputes and conflicts.
- G5.10 Demonstrate ability to work in a cooperative, collaborative way with federal, state and local intelligence, counterintelligence and law enforcement organizations.
- G5.11 Demonstrate flexibility in adapting to work in austere environments and high-threat areas.

Standard 33 maps to the following competencies.

- Written Communication
- Oral Communication
- Creative Thinking
- Analytical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Evaluation and Critique
- Laws, Policies, Procedures and Jurisdictions
- Concept Facilitation/Influencing/Negotiating
- Automated Data Systems
- Planning
- Customer Awareness
- Interpersonal Skills

CI Source Handling and Management

Standard G6 The student will demonstrate an understanding of the concepts and processes of the operation cycle for managing human CI sources.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will understand the steps involved in identifying and managing human sources of information. They will understand the importance of protecting the credibility of the source's reporting by validating the source's motivation and allegiance (asset validation).

Development

- G6.1 Assess asset's motivations for cooperating with the government as a reporting source.
- G6.2 Build confidence in assets/develop trust with sources
- G6.3 Provide operational direction for sources
- G6.4 Build strong rapport with sources to improve source responsiveness and enhance collection
- G6.5 Train sources to perform required operational tasks
- G6.6 Protect source's association with the government as a reporting asset

Validation

- G6.7
- G6.8
- G6.9

b7E

UNCLASSIFIED

Standard G6 maps to the following competencies:

- Reading Comprehension
- Written Communication
- Oral Communication
- Creative Thinking
- Analytical Thinking
- Critical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Planning
- Evaluation and Critique
- Laws, Policies, Procedures and Jurisdictions
- Concept Facilitation/Influencing/Negotiating
- Risk Management
- Customer Awareness
- Interpersonal Skills

UNCLASSIFIED

Gathering Information

Standard G7 The student will demonstrate the interpersonal, observation, and sensory skills used to gather information important to the CI mission.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will enhance their interpersonal skills in order to improve their ability to gather information through both inquiry and observation. They will understand basic methods for developing relationships to manipulate people and situations for the purpose of gathering information. Students will understand how to employ a variety of techniques to observe activities of persons or organizations that pose threats to US national security. [redacted] taught under this standard will comport with standards developed by the Community Clandestine Tradecraft Advisory Group.

b7E

Interpersonal Skills

- G7.1 Control body language to ensure actions/reactions are congruent with interviewer's role and anticipated outcomes.
- G7.2 Control interviewer's emotional tone to evoke action or reaction from subject.
- G7.3 Establish interpersonal relationship with subject/source.
- G7.4 Exploit situational conditions in order to elicit desired response.
- G7.5 Develop and identify enhancing mechanisms to motivate others.
- G7.6 Tailor interview strategies to persuade subject to work toward desired outcome.
- G7.7 Maintain professional demeanor during interaction with subject.

Inquiry

- G7.8 [redacted]
- G7.9 Employ attentive/active listening skills during interview.
- G7.10 Employ of elicitation techniques during interview.
- G7.11 [redacted]
- G7.12 Demonstrate sound interrogation skills.
- G7.13 Demonstrate sound interviewing techniques (Reid, etc.).
- G7.14 [redacted]
- G7.15 Understand the role and employ the use of interpreters during interview.

b7E

Observation

- G7.16 [redacted]
- G7.17 [redacted]
- G7.18 [redacted]
- G7.19 [redacted]

UNCLASSIFIED

G7.20

G7.21

G7.22

G7.23

G7.24

G7.25

G7.26

G7.27

b7E

Standard G7 maps to the following competencies:

- Oral Communication
- Creative Thinking
- Analytical Thinking
- Critical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Planning
- Evaluation and Critique
- Laws, Policies, Procedures and Jurisdictions
- Concept Facilitation/Influencing/Negotiating
- Automated Data Systems
- Risk Management
- Customer Awareness
- Interpersonal Skills

UNCLASSIFIED

Project Management

Standard G8 The student will understand how to plan projects and manage resources, capabilities, and processes to complete a CI operation, investigation, or analytical project.

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will understand how individual CI operational and analytical projects contribute to the strategic CI objectives of the US. With this perspective, they will gain a strategic context to the planning and conduct of individual projects. Students will understand how all CI functions and reach-back capabilities enable and enhance overall CI results.

Behavioral Outcomes

Planning

- G8.1 Demonstrate the ability to work with management teams in developing hypotheses.
- G8.2 Know how to conduct planning to advance operational objectives.
- G8.3 Understand how tactical operations and plans support national strategies.
- G8.4 Identify and know how to employ available resources.
- G8.5 Demonstrate leadership, strong initiative and ability to manage and supervise others.
- G8.6 Manage a team; provide help and assistance to team members or others when needed.
- G8.7 Plan use of manpower and resources
- G8.8 Develop and mentor others, through effective management and leadership.

Capabilities

- G8.9 Demonstrate the ability to leverage technology to advance CI activities.
- G8.10 Know reach-back capabilities and how to employ them.

Process

- G8.11 Know how to assess risks to CI operating through understanding of threats and vulnerabilities.
- G8.12 Delegate responsibility and empower others to make decisions.
- G8.13 Provide results that can be replicated.
- G8.14 Operate effectively in a dynamic, multitasking environment in the face of rapidly changing priorities.
- G8.15 Review products to ensure they arrive at logical conclusions.
- G8.16 Adapt quickly to emerging issues, priorities, and a changing work environment and respond to tasking under short and challenging deadlines.

UNCLASSIFIED

G8.17 Demonstrate effective time management, planning and organization skills.

Standard G8 maps to the following competencies:

- Oral Communication
- Creative Thinking
- Analytical Thinking
- Critical Thinking
- Decision Making
- Teambuilding/Teamwork/Collaboration
- Planning
- Evaluation and Critique
- Laws, Policies, Procedures and Jurisdictions
- Concept Facilitation/Influencing/Negotiating
- Automated Data Systems
- Risk Management
- Customer Awareness
- Interpersonal Skills

UNCLASSIFIED

Reasoning

Standard G9 The student will think creatively, analytically, and critically while collecting, analyzing, and reporting CI information.

Behavioral Outcomes

Behavioral outcomes for this standard are universal to the CI discipline at the basic level. Students will apply organized mental processes to derive meaning from collected information to anticipate events and plan for contingencies. They will use new and creative insights to apply innovative solutions to problems. Students will draw conclusions that are logical and supportable.

- G9.1 Anticipate and react to circumstances that arise during daily CI activity.
- G9.2 Demonstrate ability to conceptualize how planned activities will arrive at desired results.
- G9.3 Deduce, through logical reasoning why an activity is and/or has occurred.
- G9.4 Formulate thought patterns in a logical manner, resulting in logical conclusions.
- G9.5 Look for the unknown through abstract reasoning. Expect the unexpected from an adversary.
- G9.6 Predict and/or project conclusions as to on-going activities.
- G9.7 Develop solutions to identify problems through collaborative efforts.
- G9.8 Analyze each phase of a CI activity to consider all facts and data objectively and in a structured way.
- G9.9 Tangentially project a reason across an activity as to why it is occurring.
- G9.10 Strategically develop a "raison d'être" a particular activity fits into an adversary's strategic plans.

Standard G9 maps to the following competencies:

- Creative Thinking
- Analytical Thinking
- Critical Thinking
- Decision Making
- Evaluation and Critique
- Concept Facilitation/Influencing/Negotiating
- Risk Management
- Customer Awareness

FBI CI Strategy 2007 – 2010

~~SECRET~~

Federal Bureau of Investigation

Counterintelligence Division



DATE: 11-29-2011
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 11-29-2036

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

“FBI National Counterintelligence Strategy” 2007 - 2010

~~SECRET~~

ACLURM041915

FBI040815

~~SECRET~~

FBI CI Strategy 2007 – 2010

Table of Contents

	<u>Page</u>
I. Introduction	1
II. Implementing the CI Strategy 2007 to 2010	3
III. 2007 Strategy Model	5
IV. Strategic Focus	— 7
V. Strategic Goals	8
VI. Program Objectives/Outcomes	12
VII. Program Strategies: Field Office Activities and Accountability	16
VIII. Enabling Strategies	26
IX. Conclusion	29

~~2~~

~~SECRET~~

ACLURM041916

FBI040816

~~SECRET~~

FBI CI Strategy 2007 – 2010

I. Introduction

(U) The FBI published its first National Counterintelligence Strategy in 2002. This Strategy reflected a dramatically different direction for the Bureau's Counterintelligence Program, characterized by a commitment to confront an emerging and serious threat to the U.S. national security, and to do so multi-dimensionally. The Strategy symbolized a commitment to provide the direction, resources, and strong centralized management reflective of the number two priority of the FBI.

(U) Since the issuance of the 2002 Strategy, there have been a number of important documents promulgated throughout the Executive Branch that impact counterintelligence. First, in October 2005 the Director of National Intelligence (DNI) issued a document entitled "The National Intelligence Strategy of the United States of America." This strategy document emphasizes integration and innovation by the Intelligence Community. This was followed in March 2006, when the President of the United States issued "The National Security Strategy of the United States of America." This document complements and is consistent with the DNI's strategy. Lastly, the recently designated Counterintelligence Mission Manager, who is identified as the National Counterintelligence Executive, submitted a draft of the "Counterintelligence Strategy of the United States of America 2007," which is currently under consideration by the President. The FBI's 2002 Strategy is consistent with all the above strategy documents, and as we revise the FBI's National Strategy, the revisions will be conducted with the overarching strategies in mind, in order to promote consistency throughout the community.

(U) ~~(S)~~ The 2002 Strategy represented the first step in reorienting the Program toward focused goals and objectives. With a CI Program established in all 56 field offices, the CI Program is in the process of transformation. The program reviews recently completed in 46 offices clearly demonstrate that FBI field offices are now focused on the common priorities and objectives outlined in the 2002 Strategy.

(U) ~~(S)~~ Many of the initiatives contained in the 2002 Strategy were based on assumptions made by senior FBI Counterintelligence executives concerning the changing nature of the foreign intelligence threat. These assumptions were based on the belief that damage has been done to the United States' national security interests by the transfer of substantial critical information out of the country by foreign-sponsored intelligence networks that were not being addressed by the FBI. The 2002 Strategy asserted that the mission responsibilities of the FBI required the CI Program to work proactively with many other government agencies and the private and academic sectors, and do so in a manner that rejected its traditional reactive approach of unilateral agency action.

(U) ~~(S)~~ The Counterintelligence Division (CD) has improved its understanding of the threat, and has matured key initiatives concerning the private and public sectors. The assumptions concerning high-level foreign intelligence activities inside the United States have been corroborated and, in some cases, adjusted to reflect evidence of far greater levels of activity than originally projected.

Derived from: ~~G-3~~

Declassify on: ~~X1~~

3
~~SECRET~~

ACLURM041917

FBI040817

~~SECRET~~

FBI CI Strategy 2007 – 2010

The positive response of U.S. Government agencies, the private sector, and academia to proposed partnerships with the FBI calls for bolder leadership and more advanced objectives and priorities than those envisioned in the original 2002 Strategy. As a result, the 2007 Strategy will reflect the many changes that have occurred over the past several years. Just as the Program has evolved, so must the Strategy.

(U) ~~(S)~~ The 2007 CI Strategy stands on the shoulders of its 2002 predecessor and builds on its achievements. With this as its foundation, the 2007 Strategy consciously “raises the bar” in all Program activities. It calls for the FBI to:

- change the behavior of the most threatening foreign intelligence collectors inside the United States, as well as the American institutions and individuals exploited by those foreign collectors;
- rally the private sector and academia to form alliances with the FBI that will significantly reduce the opportunities of top priority adversaries to collect intelligence, and to substantially disadvantage those foreign adversaries’ collection plans and operations;
- reconfigure the CI Program by banding multiple FBI offices together to pool threat information and devise joint operational plans and partnering with federal agencies across the Nation through regionalized information sharing and planning;
- reinvigorate and expand National Insider Threat Program centered on the recognition and reporting system of Section 811 of the Intelligence Authorization Act of 1995; and, finally,
- enhance the national threat picture by transforming the past practice of near passive collection of foreign positive intelligence to a forward leaning proactive foreign positive intelligence collection effort spread across the Nation.

(S)

b1
b7E

II. Implementing the CI Strategy 2007 to 2010

(S)

b1
b7E

~~SECRET~~

4
ACLURM041918

FBI040818

~~SECRET~~

FBI CI Strategy 2007 – 2010

(S)

(C)

b1
b7E

(U) The 2007 Strategy also calls for integration and collaboration that reaches beyond internal operational/intelligence transformations and extends to how CD plans to collaborate with and lead other government agencies, the business sector and academia in the protection of critical national assets. [REDACTED]

b7E

[REDACTED] Information sharing is the key to the performance expected of the Working Groups. With the CI Program's adoption of the information sharing philosophy "share by rule, withhold by exception – restricting only what you must" the Working Groups will take a giant transformational step forward. With this information sharing philosophy shared by our Group partners, nearly every facet of the CI Program will be affected – from domain identification, to threat assessments, to intelligence gathering and operational planning and execution.

(S)

b1
b7E

5
~~SECRET~~

ACLURM041919

FBI040819

~~SECRET~~

FBI CI Strategy 2007 – 2010

(S)

b1
b7E

III. 2007 Strategy Model

(I) The CI strategy model clarifies the relationship between a) critically important internal capabilities and enabling structures, b) key elements of program strategy, and c) the consequences, or results that are expected from high quality performance and full capability. The FBI'S CI strategy model reinforces the notion that high value objectives are not possible without a specific type and level of performance in the program and the requisite skills, expertise, resources, and capabilities. A fully developed strategy model permits Program Managers to continually monitor strategically important aspects of the strategy, assess vulnerabilities, establish priority specific performance expectations, and provides a framework for performance measures. The FBI strategy model contains the following components:

- Strategic Focus - the overall direction of the FBI program. [redacted] as such, it should be planned and managed to have a substantial impact on the overall threat. Commitment to the success of this approach will be reflected in FBI management, engagement-accountability; actions to prioritize the application of resources; and the focus on achieving significant gains to meet our strategic goals.
- Goals/Impact - the anticipated long term results and priorities of the program. Goals generally refer to long term, government-wide accomplishments, such as preventing penetration of the intelligence community, that are beyond the capacity of any single agency to achieve. Their success places a huge premium on collaboration and partnerships. The FBI is considered successful if it significantly contributes to the government's success.
- Program Objectives/Outcomes - the specific results that can be attributed to or are caused by FBI activity. Understanding the intelligence objectives or changing behavior of industry, for example, cannot be ordered or directed. They can only be achieved with high quality performance. This category is the focus of the entire FBI Strategic Plan and its achievement and is totally dependent on how well the FBI implements the Strategy. As such, it is the primary success indicator for the CI Program.
- Program Strategies - the operational activities directed by the CI Program Managers. These reflect primary program direction and priorities to the FBI field offices - to know the Domain, collect intelligence based on requirements, target and disrupt operations - that are considered essential to achieve the program objectives. Program Managers and SACs should be held accountable to achieving the specific performance level - or game plan - associated with each program strategy element.
- Enabling Strategies - the internal capabilities required to meet the performance requirements of the program strategies. These capabilities focus on the workforce attributes and skills, the resource requirements, and the management and analytic processes that "enable" overall success of the Program

b7E

6

~~SECRET~~

ACLURM041920

FBI040820

~~SECRET~~

FBI CI Strategy 2007 – 2010

(U) The strategy model below has served as a tool for the FBI CI Program in implementing program strategies, communicating the imperative for change to internal and external stakeholders, and defining the relationship between day-to-day operational activities and the strategic objectives and goals of the Program. It has become inseparable from the Program itself and is the base of CI training provided to analysts, new CI agents, and FBI executives. This one-page strategy summary was used as the basis for the program reviews conducted of field CI programs, the reorganization of the Counterintelligence Division, and the evaluations described in the Director's Reports.

7
~~SECRET~~

ACLURM041921

FBI040821

IV. Strategic Focus

(U) The Strategic Focus represents senior management's long-term direction for the Program and sets out the highest-level impact the program is attempting to achieve. It is the final result or sum of which all of the goals, objectives, and strategies are striving to achieve.

Strategic Focus
[Redacted]

b7E

(U) The 2007 Strategy calls for a higher level of performance by focusing not simply on identifying foreign intelligence collection networks, but on reducing foreign intelligence collection opportunities, and doing so nationwide.

(C)

[Redacted]

b1
b7E

V. Strategic Goals

(C)

[Redacted]

~~SECRET~~

FBI CI Strategy 2007 – 2010

Strategic Goals

[Redacted]

b7E

Strategic Goal:

[Redacted]

(C)

[Redacted]

b1
b7E

Strategic Goal:

[Redacted]

(C)

[Redacted]

b1
b7E

Strategic Goal:

[Redacted]

(C)

[Redacted]

b1
b7E

10
~~SECRET~~

ACLURM041923

FBI040823

~~SECRET~~

FBI CI Strategy 2007 – 2010

(C)

b1
b7E

Strategic Goal:

b7E

Program Activities Associated with these Strategic Goals

- (U) ~~(C)~~ The FBI will focus its efforts and resources to achieve the Strategic Goals cited above. Making progress toward achieving these Goals requires the following FBI activities to occur over the next few years.

(C)

b1
b7E

~~SECRET~~

FBI CI Strategy 2007 – 2010

(C)



[Redacted content]

b1
b7E

Expected Impact

(C)

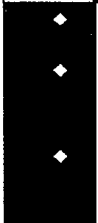
[Redacted content]

b1
b7E

VI. Program Objectives/Outcomes

(U) ~~(S)~~ Program objectives define what success looks like, and provide clarification and specificity about what a program expects to happen as a result of its implementation. However, they are not results that can be ordered; they can only be achieved by high-quality performance, focus, and effort. As such, these CI Program Objectives are the true measure of success for the FBI's CI Program.

Program Objectives/Outcomes



[Redacted content]

b1
b7E

Program Objective:

[Redacted content]

(C)

[Redacted content]

~~SECRET~~

~~SECRET~~

FBI CI Strategy 2007 – 2010

(C)



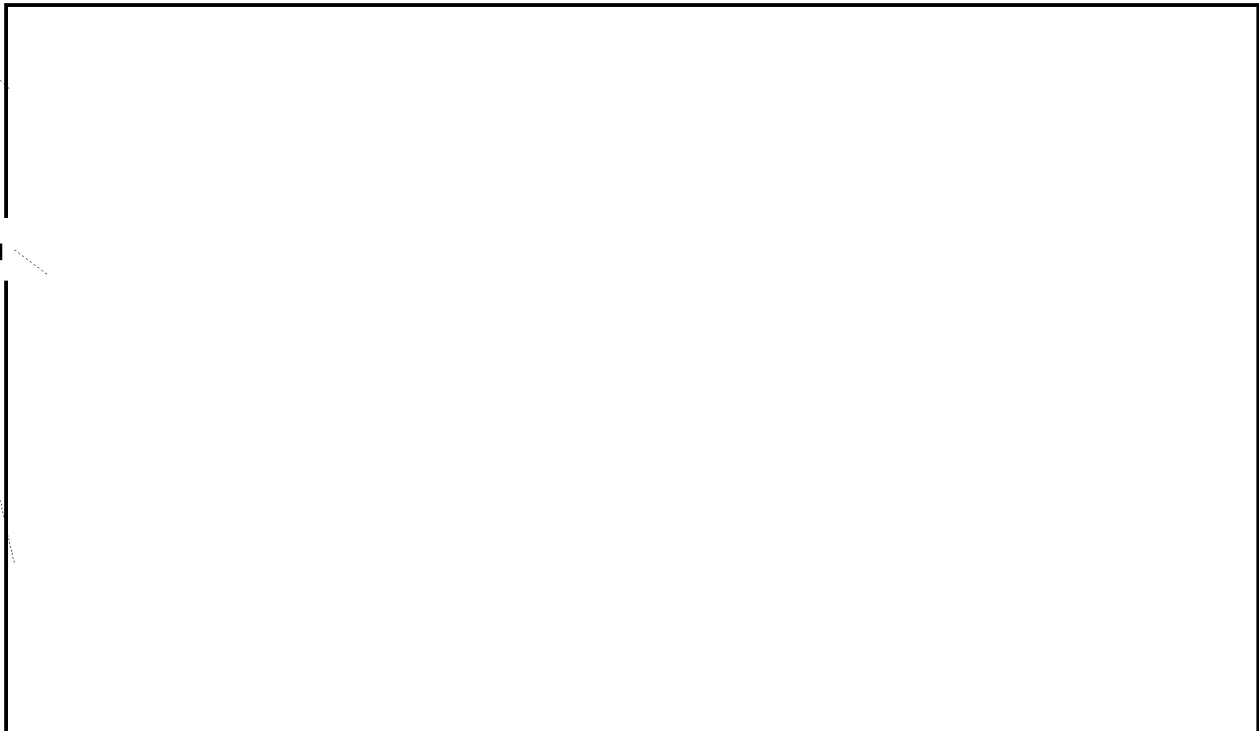
b1
b7E

Program Objective:



b7E

(C)



(C)

b1
b7E

(C)

Program Objective



(C)



b1
b7E

~~SECRET~~

FBI CI Strategy 2007 – 2010

(C)

[Redacted]

b1
b7E

(U) The foreign intelligence threat consists of three elements:

[Redacted]

[Redacted] These are the factors used to

[Redacted]

[Redacted]

b7E

Program Activities Associated with these CI Objectives

(S)

[Redacted]

b1
b7E

Expected Impact

(C)

[Redacted]

b1
b7E

14
~~SECRET~~

ACLURM041927

FBI040827

~~SECRET~~

FBI CI Strategy 2007 – 2010

VII. Program Strategies: Field Office Activities and Accountability

(U) Program Strategies are the specific activities of a strategy that provide the means by which a program will achieve its program objectives. Success for a program will be totally dependent on the speed and effectiveness with which these program strategies are implemented.

The CI Program Strategies are now recognized throughout HQ and the field as key elements of the CI Program and remain intact in the 2007 Strategy. However, two Program Strategies are being added to give greater prominence to (1) [REDACTED] and (2) [REDACTED]

b7E

Program Strategies

◆	
◆	
◆	
◆	
◆	
◆	

b7E

Program Strategy:

--

--

b1
b7E

(C)

15
~~SECRET~~

ACLURM041928

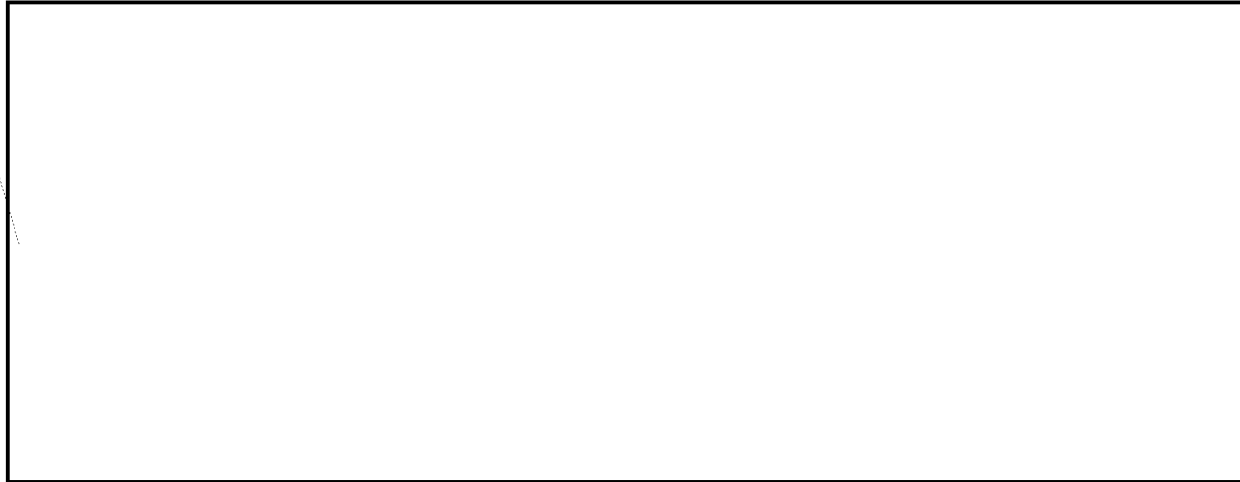
FBI040828

~~SECRET~~

FBI CI Strategy 2007 – 2010

Program Activities

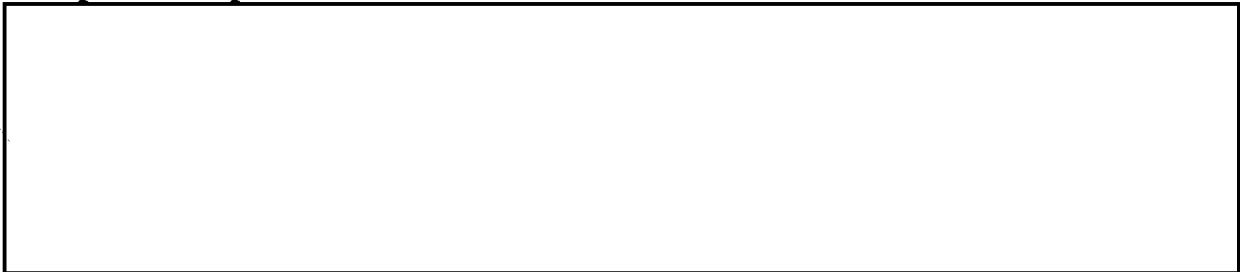
(C)



b1
b7E

Expected Impact

(C)



b1
b7E

Program Strategy: Interface with the Domain—Educate and Collaborate with Businesses, Universities, and other Private Sector Entities that may be Targeted by Foreign Intelligence Collectors.

(C)



b1
b7E

Program Activities

(C)



b1
b7E

16
~~SECRET~~

ACLURM041929

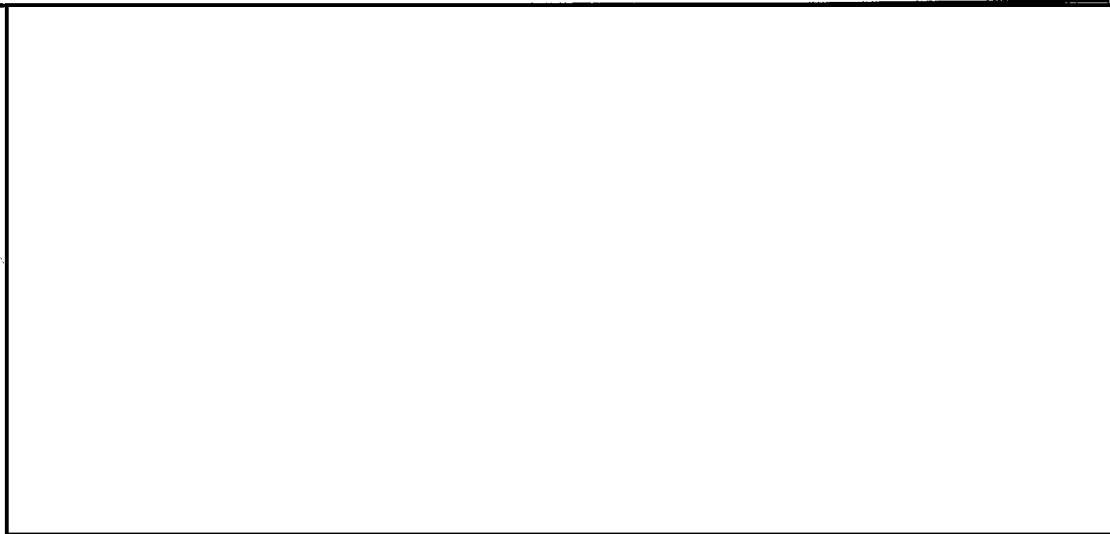
FBI040829

~~SECRET~~

FBI CI Strategy 2007 – 2010

(C)

➤
➤
➤
➤
➤



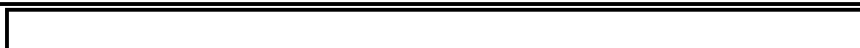
b1
b7E

Expected Impact

(C)



Program Strategy:



b1
b7E

(C)



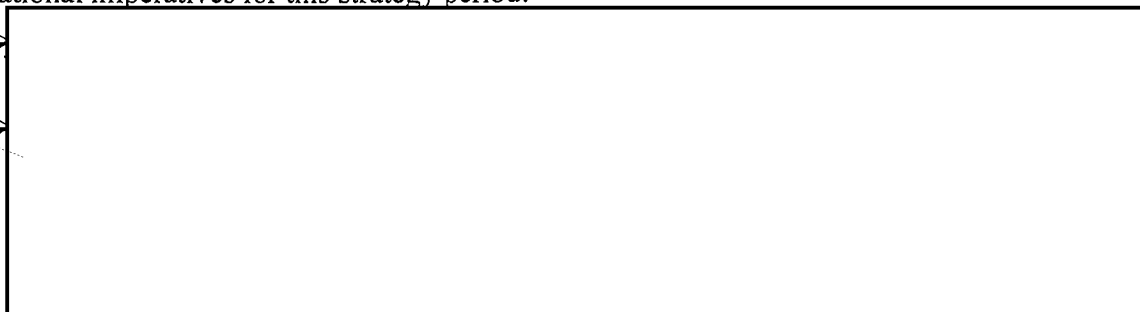
Program Activities

(U)

~~(C)~~ Under the 2007 CI Strategy, HQ CD program managers and field executives have two clear operational imperatives for this strategy period:

➤
➤

(C)



b1
b7E

~~17
SECRET~~

ACLURM041930

FBI040830

~~SECRET~~

FBI CI Strategy 2007 – 2010

Expected Impact

[Redacted]

b7E

Program Strategy:

[Redacted]

[Redacted]

Program Activities

[Redacted]

(C)

b1
b7E

~~18
SECRET~~

ACLURM041931

FBI040831

~~SECRET~~

FBI CI Strategy 2007 – 2010

Expected Impact

[Redacted]

Program Strategy:

[Redacted]

[Redacted]

b7E

Program Activities

[Redacted]

(C)

b1
b7E

~~SECRET~~

FBI CI Strategy 2007 – 2010

(C)

b1
b7E

Expected Impact

b7E

Program Strategy:

(U) As a member of the U.S. Intelligence Community, the CI Program is committed to responding to National Intelligence Requirements as identified by the Office of the Director of National Intelligence (ODNI) and the FBI NSB Directorate of Intelligence (DI). Post 9/11, all intelligence agencies must respond to national requirements where they can bring significant value and advance the national interest. The CI Program will take a proactive approach to fulfilling national requirements, and do so through targeted operations and sources.

Program Activities

(U) The purpose of these program actions is to contribute to the National Intelligence Strategy of the United States.

- Translate all National Intelligence Priority Framework (NIPF) and FBI priority program requirements into a format that can be easily understood by field intelligence collectors; and,

➤

b7E

Expected Impact

(U) The expected impact from these program actions, as well as others described in this Strategy, is a sustained increase in the CI Program's contribution to the National Intelligence Strategy of the United States. Having a broader understanding of the national collection requirements allows the CI Program to mobilize its agents and analysts, focus its efforts, and take advantages of every opportunity to collect additional information to the benefit of the entireUSIC.

20
~~SECRET~~

ACLURM041933

FBI040833

VIII. Enabling Strategies

(U) Enabling strategies identify the core internal management requirements necessary for the organization. They are the foundation of the entire strategic framework.

Enabling Strategies

♦ <u>Workforce</u>	♦ <u>Resources</u>	♦ <u>Intelligence</u>	♦ <u>Management Accountability</u>
Training	Distribution of staff	Asset validation	SACs
Experience		Information sharing	HQ Program Managers
Continuity		Access to data	

Enabling Strategy: Workforce—Training, Experience, and Continuity.

(U) ~~(C)~~ Training this newly assigned and inexperienced workforce has been a major focus of the Program. [REDACTED]

b7E

Program Activities

(U) The Program can only make progress toward a **professional** and **proficient** workforce if the training effort is matched by a commitment to personnel continuity within the CI Program. During the next few years, the Program will:

- Train all CI agents and Intelligence Analysts in [REDACTED] to enable them to fulfill the high demands of the 2007 Strategy;
- Encourage field executives to assign CI experienced personnel to their CI Programs and where CI experience is unavailable assign experienced investigative and analytical personnel; and,
- Hold field executives accountable for the continuity of personnel within their CI Programs.

b7E

Expected Impact

(U) The expected impact from these program actions is a workforce that is professionally prepared, and equal to the challenges of the 2007 Strategy.

Enabling Strategy: Resources—Distribution of Staff.

(U) ~~(C)~~ Distribution of Staff: In 2002, the FBI made [REDACTED] This commitment has proved pivotal to the Program's appreciation of the size and complexity of the foreign intelligence threat we face today. With the demands of the 2007 Strategy, the Program distribution of staff must be taken to the next level. CD requires a new Program Management approach to the Program—to include a new planning cycle for field office resource allocation and budgeting.

b7E

~~SECRET~~

FBI CI Strategy 2007 – 2010

Program Activities

(U) ~~(C)~~ The following program actions are essential to realizing this enabling strategy.

(C)

➤ Establish a process and annual schedule for [redacted] performance expectations, training and development, and data requirements, among other Program necessities; and,

➤ Review the distribution of CI resources to provide counterintelligence coverage in resident agencies.

b1
b7E

Expected Impact

(U)

~~(C)~~ The expected impact from these program actions is the establishment of a comprehensive Program Management regimen in CD.

Enabling Strategy: Intelligence—Asset Validation, Information Sharing, and Internal Access to Data.

(U) ~~(C)~~ Asset Validation: In 2002, there was no formalized process at FBI Headquarters to independently validate the authenticity and bona fides of CI assets. Due to growing concerns about the quality and credibility of sources, and the discovery of irregularities in some highly visible investigations, CD launched several initiatives to address these concerns. [redacted]

b7E

(U) ~~(C)~~ Information Sharing: Prior to 2001, information sharing was a limited Program enterprise, relegated to sharing investigative information on a case-by-case basis with individual agencies. In the post 9/11 era, and with the creation of the Office of the Director of National Intelligence and the FBI's own Directorate of Intelligence, the CI Program must significantly increase its information sharing. The 2007 Strategy candidly notes that the CI Program success is heavily dependent on collaborations and partnerships, both of which are built on information that is shared, relevant, and timely.

(U) ~~(C)~~ Internal Access to Data: Membership in the USIC requires FBI field offices to be able to electronically communicate with other community members and access their information, just as other members must communicate with and access FBI information. Such community discourse is not broadly possible with FBI field offices currently. Access to such systems as [redacted] and even the Internet, is neither broad nor generally accessible enough for the FBI field office personnel to take part in the professional, free exchange of information within the community.

b7E

22
~~SECRET~~

ACLURM041935

FBI040835

FBI CI Strategy 2007 – 2010

Program Activities

(U) The following program actions and others described in this Strategy are essential to realizing this enabling strategy. During the next few years, the Program will:

-
-
- Produce and disseminate finished intelligence that informs, warns or places disparate pieces of intelligence into a greater context, and,
- Continue current efforts to broadly increase access to relevant USIC databases and electronic communications systems.

b7E

Expected Impact

(U) The expected impact from these program actions is the production and dissemination of Program intelligence that serve their intended function: “reliable information specifically tailored to serve as a prelude to a decision or action.”

Enabling Strategy: Management Accountability – SAC and Headquarters Program Managers Responsibilities

(U) ~~(C)~~ **Headquarters Program Managers:** Headquarters Program Managers are responsible for the effective execution of all six Program Strategies and all four of the Enabling Strategies. Program Managers are responsible for devising field guidance which comports with the National Strategy for CI and for furnishing direction to the field concerning all aspects of the Strategy. It is within the authority and command capacity of Program Managers to shut down field activities that do not directly support the National Strategy. Headquarters Program Managers are held accountable for knowing all individual field activities and are the final arbiters as to whether or not a field operation or initiative is furthering the National Strategy.

(U) ~~(C)~~ **SAC Responsibility:** SACs are responsible for the effective execution of all six Program Strategies in the 2007 National CI Strategy and three of the four Enabling Strategies, i.e., Workforce Expertise, Intelligence and Management Accountability. These activities are within the SACs authority and command capacity and as a result can be “directed” by the SAC to be done. Because these activities are within the field executive’s control, SACs will be held accountable for their execution.

IX. Conclusion

(U) The 2007 CI Strategy establishes a roadmap for the next few years that “raises the bar” for Program performance. It calls for the FBI to think differently about the CI Program, plan differently for the CI Program, and act differently in executing the CI Program. It calls for the FBI to change the behavior of the most threatening foreign intelligence collectors inside the

~~SECRET~~

FBI CI Strategy 2007 – 2010

United States, and change the behavior of American institutions and individuals who are exploited and victimized by those foreign collectors. It calls for the FBI to collaborate and partner with other U.S. Government agencies, the private sector, and academia in unprecedented ways to reduce the opportunities of top priority adversaries to collect intelligence. It calls for the FBI to be programmatically creative in carrying out its intention to substantially disadvantage the collection plans and operations of its highest priority adversaries, whether those operations are traditionally [REDACTED]

[REDACTED] It also calls for the FBI to be proactive about detecting and deterring the most damaging of all spies – the trusted Insider.

b7E

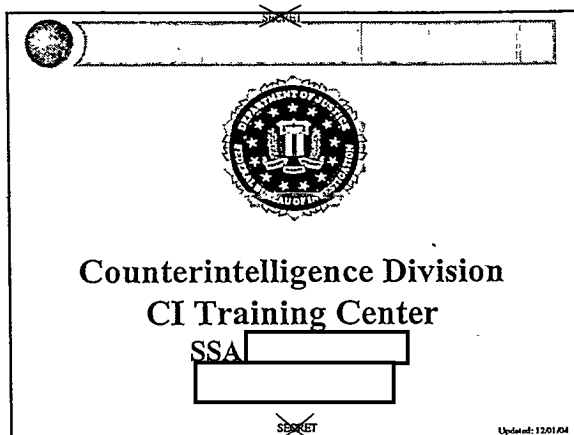
(U) The 2007 Strategy explicitly recognizes the CI Program's obligation to share information as part of its day-to-day business and it declares the Program's obligation to respond to National Intelligence Requirements to preserve the national security and economic interests of the United States.

24
~~SECRET~~

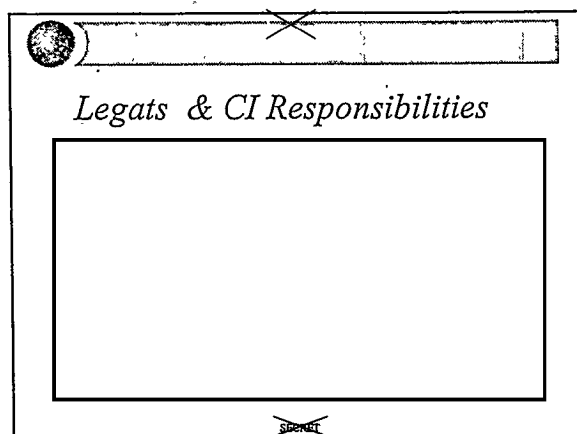
ACLURM041937

FBI040837

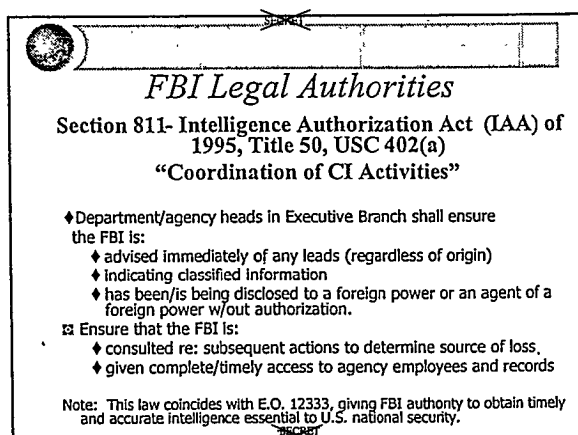
DECLASSIFIED BY 65179 DMH/STW
ON 12-07-2011



b6
b7C



b7E



Section 811-Failed Polygraphs

♦ Past Cases:

~~SECRET~~

b6
b7C

Five Elements of CI Operational Strategy

~~SECRET~~

b7E

PAST CASES

~~SECRET~~

b6
b7C

PAST CASES

~~SECRET~~

b6
b7C

PAST CASES

~~SECRET~~

b6
b7C

PAST CASES

~~SECRET~~

b6
b7C

~~SECRET~~

PAST CASES

~~SECRET~~

b6
b7C

~~SECRET~~

PAST CASES

~~SECRET~~

b6
b7C

~~SECRET~~

PAST CASES

~~SECRET~~

b6
b7C

~~SECRET~~

Counterespionage Priorities

~~SECRET~~

b7E

~~SECRET~~

STRATEGIC OBJECTIVES

~~SECRET~~

b7E

~~SECRET~~

Overseas Espionage Investigations

Section 603 of the IAA of 1990
(Title 28 USC Section 533)

- ♦ FBI supervises espionage investigations involving persons employed by or assigned to U.S. diplomatic missions abroad (to include: DOD personnel & FSNs).
- ♦ WFO is the Office of Origin for all overseas espionage investigations.
- ♦ These investigations are approved by the DCI and coordinated with CIA, USDS and Chief of Mission.

~~SECRET~~

~~SECRET~~

IAA of 2001: Section 605, "Coordination of Counterintelligence with the FBI"

Two Key Provisions

- ◆ FBI notifies affected Executive Branch heads of departments or agencies when an investigation is opened regarding their employees.
 - Departments/agencies may not polygraph, interrogate or take other actions to alert the employee without prior coordination with the FBI.
- ◆ FBI Director shall provide department or agency heads a written assessment on how their actions can impact the CI investigation.

~~SECRET~~

~~SECRET~~



**Counterintelligence Division
CI Training Center (CITC)**

SSA

~~SECRET~~ Updated: 12/01/04

b6
b7c

DATE: 01-06-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-06-2037

7/19/2011

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Counterintelligence
Division
Operational
Training Unit



Everything you
want to know,
and more.....

The FBI is NOT...

- The National Police
- An Intelligence Service

The FBI Is...

- A Law Enforcement Agency
- A Counterintelligence/
Counterterrorism Service



FBI's Ten-Point List of Priorities

- Counterterrorism
- Counterintelligence / Espionage
- Cyber Attacks / High Technology Crimes
- Public Corruption Investigations
- Civil Rights Investigations



Ten-Point List of Priorities (Continued)

- Transnational & National Criminal Organizations
- Major White Collar Crime
- Significant Violent Crime
- Support Federal, State, Local & International Partners
- Upgrade the FBI's Technical Capabilities



What Do We Do?

- As a Law Enforcement Agency with broad federal criminal jurisdiction, the FBI is directed against national criminal activity (criminal enterprises, public integrity, etc.)

What Do We Do?

- As a Counterintelligence/ Counterterrorism Service the FBI is authorized to prevent and defeat intelligence and terrorist activities conducted by individuals and organizations adversarial to U.S. interests.

What Do We Do?

- FBI is lead Counterintelligence and Counterterrorism Agency in U.S.



~~SECRET~~

National Security Programs



1. Foreign Counterintelligence
2. International Terrorism
3. Domestic Terrorism

Types of NSP Investigations

- Intelligence Gathering
 - Foreign Counterintelligence
 - Counterterrorism
- Criminal Investigations
 - Espionage
 - Economic Espionage
 - Sabotage
 - Bombings, etc.

U.S. Intelligence Community

- As FBI employees, you are members of the U.S. Intelligence Community (USIC).

U.S. Intelligence Community

- Other Members of USIC:
 - 
 - Departments of State, Energy & Treasury
 - Department of Defense
 - 
 - Air Force, Army, Navy, Marine Corps Intelligence components

What Do We Do?

- As a Counterintelligence/Counterterrorism Service the FBI is authorized to prevent and defeat intelligence and terrorist activities conducted by individuals and organizations adversarial to U.S. interests.



How Do We Do It?

- How do we prevent and defeat?



b7E

How Do We Do It?



How Do We Do It?



How Do We Do It?



(S)

b1
b7E

~~SECRET~~

7/19/2011

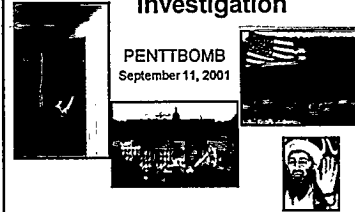
How Do We Do It?



How Do We Do It?



The Current FBI IT Investigation



b7E

Notable FBI FCI, IT & DT Investigations



Information Security

Clearance + Need to Know =

Access

to Classified Information

Personnel Security



b1
b7E

National Security

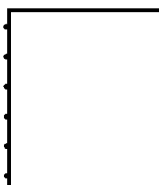
• Last 10 years -

Documented recruitment attempts of students

Documented cases of an FBI employee providing classified information to a FIS



Steps in the Recruitment Process



b7E

~~SECRET~~

7/19/2011

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-29-2011 BY 65179 DMH/STW

Intelligence Authorization Acts

- EO 12333
- 811
- 603
- 2.5
- Third Agency Rule

Predication

Legal Issues

Legal Issues Continued...

b7E

~~SECRET~~

DATE: 01-06-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-06-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Counterintelligence Operations

(S) General CI Review and
Mindset of an [redacted]

SSA [redacted]
[redacted] November 2004

SECRET

FBI CI Responsibility

- Unique Jurisdiction for CI investigations in U.S.
- Sole coordinating responsibility for FI collection within U.S. per EO 12333.
- Unique Jurisdiction for Criminal Espionage Investigations.

SECRET

b1
b6
b7C
b7E

(S)

(S)

(S)

(S)

(S)

b1
b7E

~~SECRET~~

copy

~~SECRET~~

DISCOVERY REQUEST MATERIAL

DATE: 12-06-2011
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 12-06-2036

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR

MARCH 10-14, 2008

~~SECRET~~

~~SECRET~~

CI Executive Management Seminar
March 10-14, 2008

Last Name First Field Office

Status

Named Legat Copenhagen

Sept 28 - Oct 1

Sept 28 - Oct 1

either date works

Aug 31- Sept 3

Sept 28 - Oct 1

b6

b7C

(S)

either date works

Sept 28 - Oct 1

Sept 28 - Oct 1

POC

b1

b6

b7C

b7E

~~SECRET~~

Counterintelligence Training Center

Class Name: CI Executive Management Seminar 08-01

Class Dates: 03/10-14/2008

Last Name	First Name	MI	SSN	Agency
-----------	------------	----	-----	--------

(S)

(S)

(S)

b1
b6
b7C
b7E

Staff:

(S)

b1
b6
b7C
b7E

Counterintelligence Training Center						7/13/2011		
Please complete this form to [] to insure training credit is recorded.								
Class Name:	CI Executive Management Seminar 08-01			TR #	[]			Virtual Academy: yes or no
Travel Dates:	3/9/2008							* required information -
Class Dates:	03/10-14/2008							
Class Location:	[]							
Class Coordinator:	[]			Section/Unit Sponsor:	[]			
Notes:								
*	*	*	*	*	*			
Last Name	First Name	MI	Title	SSN	FO	Telephone	Notes	Secretary

Counterintelligence Training Center						7/13/2011	
Please complete this form to [redacted] to insure training credit is recorded.							
Class Name:		CI Executive Management Seminar 08-01				TR # [redacted]	
Travel Dates:		3/9/2008				Virtual Academy:	
Class Dates:		03/10-14/2008				* required inform	
Class Location:							
Class Coordinator:						Section/Unit Sponsor:	
Notes:							
*		*		*		*	
Last Name		First Name		MI		Title	
SSN		FO		Telephone		Notes	

b1
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 02/29/2008

Date: 01/22/2008

To: All Field Offices

Attn: SACs
ASACs
Training Coordinators

b6
b7C
b7E

From: Counterintelligence Division

Contact: SSA [REDACTED]

Approved By: [REDACTED]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-06-2011 BY 65179 DMH/STW

Drafted By: [REDACTED] :kd

Case ID #: [REDACTED]

Title: COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR;
COUNTERINTELLIGENCE DIVISION;
COUNTERINTELLIGENCE TRAINING CENTER (CITC);
MARCH 10 - 14, 2008;
[REDACTED]

Synopsis: To advise receiving offices of captioned seminar and to provide administrative information.

Details: The Federal Bureau of Investigation (FBI) National Strategy for Counterintelligence (CI) mandates an increased focus on both the professionalization of the FBI CI workforce and the training required to establish that professionalized cadre. As part of this training, the Counterintelligence Division (CD) has developed and mandated a CI Executive Management Seminar for all Special Agents-in-Charge (SACs) and Assistant Special Agents-in-Charge (ASACs) who are overseeing CI operations, have not already attended this seminar, and are not considered proficient in CI. The seminar will focus on various topics outlined in the National Strategy for CI.

CI proficiency for Executive Managers is defined as three (3) years in the CI program and two (2) CI courses of any kind, either FBI or United States Intelligence Community (USIC) sponsored.

b7E

While the seminar is open to all field executives, preference will go to those executives assigned to the CI program. The seminar is being held at [REDACTED]

To: All Field Offices From: Counterintelligence Division
Re: [REDACTED] 01/22/2008

b7E

[REDACTED] Space is limited to 30 seats.

In an effort to foster continuing collaboration with our USIC partners, CITC is requesting all SACs and ASACs registering for this course nominate an equivalent executive (GS-15/SES) from the USIC, with whom you have continuing contact and would benefit from this training. This is only a nomination and final selection will be made by the CD. While the FBI will cover materials and course fees for the USIC attendees, the travel and per diem costs must be incurred by their individual agencies.

COURSE LOCATION AND DURATION

The CI Executive Management Seminar will be held at the [REDACTED]. The seminar will start promptly at 8:30 AM on Monday, March 10, 2008 and will end at approximately 10:00 AM on Friday, March 14, 2008.

b7E

Sunday, March 9, 2008 is the designated travel day for this seminar. If possible, no travel arrangements should be made with a departure time prior to the morning of Friday, March 14, 2008.

On Tuesday, March 11, 2008, there will be an evening event at the [REDACTED]. Transportation to and from this event will be provided. As food will be provided, per diem costs for dinner must be deducted from your individual vouchers. The per diem amount to be deducted is \$31.00.

b7E

Attendees should make reservations at the [REDACTED]. The FBI has reserved a block of rooms under the name [REDACTED]. The hotel is located at [REDACTED]. The telephone number for reservations is [REDACTED].

b7E

If you are choosing to stay at another area hotel, you are reminded, due to high occupancy rates, U.S. Government per diem rate rooms may be unavailable. It is requested that attendees make reservations at the [REDACTED] as soon as possible.

VOUCHERS

To: All Field Offices From: Counterintelligence Division
Re: [REDACTED] 01/22/2008

b7E

Vouchers for travel relative to this training will be charged to a travel authorization number provided at a later date. Rental vehicles will not be authorized for this TR number. The cost of rental vehicles must be carried by the individual attendee or the attendee's field office. CD Supervisors or Third Party Draft officials shall not authorize any vehicle rentals under the provided TR number.

The maximum allowance for lodging in the Arlington, VA area while on U.S. Government official business is \$201.00 per night. The allowance for miscellaneous and incidental expenses is \$64.00 per day.

TRAVEL AND TRANSPORTATION

If traveling by air, attendees are encouraged to utilize Ronald Reagan Washington National Airport. There will be complimentary shuttle service to the hotel. While at the hotel, there is complimentary shuttle service to and from the Crystal City shops, the Washington D.C., metro system and the

b7E

ATTENDANCE

As is customary at in-service training, attendance is mandatory for all seminar sessions. If an absence is unavoidable, contact the [REDACTED] at [REDACTED]. This requirement is to ensure that the attendee is in an on-duty status and will provide the attendee the appropriate protection in the event of an emergency.

b6
b7C

IN-SERVICE TRAINING AND REGISTRATION

Virtual Academy and FBI e-mail will be the mechanism to register for this seminar.

The course is listed as the CI Executive Management Seminar in the Virtual Academy.

CITC requests that all attendees complete the following as soon as possible:

- (1) Register through the Virtual Academy.
- (2) Via internal FBI e-mail to

To: All Field Offices From: Counterintelligence Division
Re: [REDACTED] 01/22/2008

b6
b7C
b7E

SSA [REDACTED] CITC, CD, using
the subject "*CI Executive Management Seminar*",
provide the following information:

- (a) Official Bureau Name and Title
- (b) Name preferred for classroom strip
- (c) SSAN
- (d) Field Office Assignment and telephone
number(s) for further contact
- (e) Name and contact information for USIC
personnel you are nominating for
attendance to this course

MISCELLANEOUS

Professional business attire is appropriate for this
seminar.

Any employee selected to attend this in-service who may
be in need of a special accommodation (i.e., sign language
interpreter; audio loop; personal assistant; large print
materials; etc.) should contact [REDACTED]
[REDACTED] as soon as possible.

Any questions concerning this seminar should be
directed to the following CITC personnel:

b6
b7C

[REDACTED]

To: All Field Offices From: Counterintelligence Division
Re: [REDACTED] 01/22/2008

b7E

LEAD(s) :

Set Lead 1: (Action)

ALL RECEIVING OFFICES

(U) 1. Division Training Coordinators need to input the attendees' information into the Virtual Academy under the *CI Executive Management Seminar*.

(U) 2. Attendees need to provide via the internal FBI email the following information to SSA [REDACTED] CITC, CD, using the title "*CI Executive Management Seminar*" no later than February 29, 2008:

b6
b7C

- (a) Official Bureau Name and Title
- (b) Name preferred for classroom strip
- (c) SSAN
- (d) Field Office Assignment and telephone number(s) for further contact
- (e) Name and contact information for USIC personnel you are nominating for attendance to this course

♦♦

~~SECRET~~



Counterintelligence Executive Management Seminar

March 10-14, 2008

Monday, March 10th

8:30am - 8:45am

Welcome to [redacted]
Security Briefing

Coordinator

[redacted]

b6
b7C
b7E

8:45am - 10:00am

Counterintelligence Division

Daniel Lee Cloyd, Assistant Director
Kevin Favreau, Deputy Assistant Director
Counterintelligence Division

10:00am - 10:15am

Break

10:15am - 12:15pm

Introduction to Counterintelligence and Legal Authorities

[redacted]
National Security Law Branch

b6
b7C

12:15pm - 1:00pm

Lunch

1:00pm - 1:45pm

Understanding the Threat

Virginia Bollinger, Section Chief, Analytical Section

1:45pm - 2:45pm

What to do about the Threat: CD Section Battle Plans

James Casey, Section Chief, Eurasia Section
Gerald Rose, Section Chief, Global Section
Bruce Carlson, Section Chief, East Asia Section

2:45pm - 3:00pm

Break

3:00pm - 4:00pm

What to do about the Threat: CD Section Battle Plans (continued)

James Casey, Section Chief, Eurasia Section
Gerald Rose, Section Chief, Global Section
Bruce Carlson, Section Chief, East Asia Section

4:00pm

Wrap-up

~~SECRET~~



Counterintelligence Executive Management Seminar

March 10-14, 2008

Tuesday, March 11th

8:30am - 10:30am *Domain Initiatives: Engaging in Strategic Partnerships;
Working with the Academic and Business Alliances*

Thomas J. Mahlik, Section Chief

[Redacted]

CI Strategy and Domain Section

b6
b7C

10:30am - 10:45am *Break*

10:45am - 11:45am *Regional Counterintelligence Working Groups: Best Practices*

Thomas J. Mahlik, Section Chief

[Redacted]

CI Strategy and Domain Section

b6
b7C

11:45am - 12:30pm *Lunch*

12:30pm - 1:30pm *Counterespionage Issues*

[Redacted]

1:30pm - 2:30pm

[Redacted]

[Redacted]

b6
b7C
b7E

2:30pm - 3:30pm

Wrap-up, board bus at

[Redacted]

3:15pm - 5:00pm

Self-guided tour of

[Redacted]

5:00pm - 6:30pm

Reception

6:30pm - 8:30pm

[Redacted]

(S)

b1
b6
b7C
b7E

8:30pm - 9:00pm

Return travel to

[Redacted]

Counterintelligence Executive Management Seminar

March 10-14, 2008

Wednesday, March 12th

8:30am - 9:30am [redacted] ***Resources and Training Simulation***
Peter Georgacopoulos, Section Chief
Operations Support to the IC, Surveillance, and Training Section
[redacted]
Counterintelligence Training Center

b6
b7C
b7E

9:30am - 10:30am ***Confidential Human Source Validation: Vital & Essential***
Timothy J. Healy, Deputy Assistant Director
Directorate of Intelligence

10:30am - 10:45am ***Break***

10:45am - 11:45pm ***Confidential Human Source Validation: Vital & Essential***
[redacted]

11:45pm - 12:30pm ***Lunch***

12:30pm - 1:45pm ***The Value of Sophisticated Operations and Best Practices***
[redacted]

b6
b7C

1:45pm - 2:15pm ***National Security Branch***
[redacted]

2:15pm - 2:30pm ***Break***

2:30pm - 4:00pm ***Round Table Discussion, Best Practices***
Seminar Attendees

4:00pm ***Wrap up***



Counterintelligence Executive Management Seminar

March 10-14, 2008

Thursday, March 13th

8:30am - 9:15am *Office of the Director of National Intelligence*
[redacted] to Assistant Deputy Director of
National Intelligence for Humint, Deputy Directorate for Collections
Mr. Clay Cowart, Assistant Deputy Director of National Intelligence
for [redacted] Deputy Directorate for Collections

9:15am - 10:15am *Cyber Division*
James E. Finch, Assistant Director

10:15am - 10:30am *Break*

10:30am - 11:30am *Weapons of Mass Destruction Directorate: Counterproliferation*
Vahid Majidi, Assistant Director

11:30am - 12:15pm *Lunch*

12:15pm - 1:15pm *Counterterrorism Division*
Charles Frahm, Deputy Assistant Director

1:15pm - 2:00pm *Closing Remarks*
Kevin Favreau, Deputy Assistant Director, Counterintelligence
Division

2:00 pm *Wrap up*

b6
b7c

~~SECRET~~

DISCOVERY REQUEST MATERIAL

DATE: 12-06-2011
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 12-06-2036

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR

SEPTEMBER 22-26, 2008

~~SECRET~~

Counterintelligence Training Center						7/13/2011	
Please complete this form to [] to insure training credit is recorded.							
Class Name:	CI Executive Management Seminar 08-01 TR # []				Virtual Academy yes or no		
Travel Dates:	9/21/2008				* required information -		
Class Dates:	09/22-25/2008						
Class Location:	SIOC						
Class Coordinator:	[]			Section/Unit Sponsor:	[]		
Notes:							
*	*	*	*	*			
Last Name	First Name	MI	Title	SSN	FO	Telephone	Notes
[]							

b1
b6
b7C
b7E

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 09/12/2008

Date: 07/02/2008

To: All Field Offices

Attn: SACs
ASACs
Training Coordinators

From: Counterintelligence
Counterintelligence Training Center
Contact: SSA

Approved By:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-06-2011 BY 65179 DMH/STW

b6
b7C
b7E

Drafted By:

Case ID #: (Pending)

Title: COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR;
COUNTERINTELLIGENCE DIVISION;
COUNTERINTELLIGENCE TRAINING CENTER (CITC);
SEPTEMBER 22 - 26, 2008;

Synopsis: To advise receiving offices of captioned seminar and to provide administrative information.

Details: The Federal Bureau of Investigation (FBI) National Strategy for Counterintelligence (CI) mandates an increased focus on both the professionalization of the FBI CI workforce and the training required to establish that professionalized cadre. As part of this training, the Counterintelligence Division (CD) has developed and mandated a CI Executive Management Seminar for all Special Agents-in-Charge (SACs) and Assistant Special Agents-in-Charge (ASACs) who are overseeing CI operations, have not already attended this seminar, and are not considered proficient in CI. The seminar will focus on various topics outlined in the National Strategy for CI.

CI proficiency for Executive Managers is defined as three (3) years in the CI program and two (2) CI courses of any

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 07/02/2008

b7E

kind, either FBI or United States Intelligence Community (USIC) sponsored.

While the seminar is open to all field executives, preference will go to those executives assigned to the CI program. The seminar is being held at the [REDACTED]. Space is limited to 30 seats.

In an effort to foster continuing collaboration with our USIC partners, CITC has opened this seminar to the USIC. CITC will be working with the training divisions of each USIC agency for attendees from the USIC. However, if you are attending this course and would like to nominate an equivalent executive (GS-15/SES) from the USIC, with whom you have continuing contact and would benefit from this training, please forward the name to CITC with your registration information. This is only a nomination and final selection will be made by the CD through liaison with the USIC agency's training office. While the FBI will cover materials and course fees for the USIC attendees, the travel and per diem costs must be incurred by their individual agencies.

COURSE LOCATION AND DURATION

The CI Executive Management Seminar will be held at the [REDACTED]. The seminar will start promptly at 8:30 AM on Monday, September 22, 2008 and will end at approximately 10:00 AM on Friday, September 26, 2008.

b7E

Sunday, September 21, 2008 is the designated travel day for this seminar. If possible, no travel arrangements should be made with a departure time prior to the morning of Friday, September 26, 2008.

On Wednesday, September 24, 2008, there will be an evening event at the [REDACTED]. Transportation to and from this event will be provided. As food will be provided, per diem costs for dinner must be deducted from your individual vouchers. The per diem amount to be deducted is \$31.00.

b7E

Attendees should make reservations at the [REDACTED]. The FBI has reserved a block [REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 07/02/2008

of rooms under the name "Executive Seminar." The hotel is located at [REDACTED]. The telephone number for reservations is [REDACTED].

b7E

If you are choosing to stay at another area hotel, you are reminded, due to high occupancy rates, U.S. Government per diem rate rooms may be unavailable. It is requested that attendees make reservations at the [REDACTED] as soon as possible. The hotel is holding the rooms at the government per diem rate until August 29, 2008.

VOUCHERS

Vouchers for travel relative to this training will be charged to a travel authorization number TR [REDACTED]. Rental vehicles will not be authorized for this TR number. The cost of rental vehicles must be carried by the individual attendee or the attendee's field office. Third Party Draft officials shall not authorize any vehicle rentals under the provided TR number.

b7E

The maximum allowance for lodging in the Arlington, VA area while on U.S. Government official business is \$201.00 per night. The allowance for miscellaneous and incidental expenses is \$64.00 per day.

TRAVEL AND TRANSPORTATION

If traveling by air, attendees are encouraged to utilize Ronald Reagan Washington National Airport where a shuttle bus will take you to the hotel. The Washington, D.C. metro system yellow or blue line will also take attendees from the airport to the Crystal City stop. The Crystal City Shops has an underground tunnel to that hotel and the [REDACTED].

b7E

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 07/02/2008

b6
b7C
b7E

ATTENDANCE

As is customary at in-service training, attendance is mandatory for all seminar sessions. If an absence is unavoidable, contact the [REDACTED] at [REDACTED]. This requirement is to ensure that the attendee is in an on-duty status and will provide the attendee the appropriate protection in the event of an emergency.

IN-SERVICE TRAINING AND REGISTRATION

Virtual Academy and FBI e-mail will be the mechanism to register for this seminar.

The course is listed as the CI Executive Management Seminar in the Virtual Academy.

CITC requests that all attendees complete the following as soon as possible:

- (1) Register through the Virtual Academy.
- (2) Via internal FBI e-mail to SSA [REDACTED] CITC, CD, using the subject "CI Executive Management Seminar", provide the following information:
 - (a) Official Bureau Name and Title
 - (b) Name preferred for classroom strip
 - (c) SSAN
 - (d) Field Office Assignment and telephone number(s) for further contact
 - (e) Name and contact information forUSIC personnel if you are nominating one for attendance to this course

b6
b7C

MISCELLANEOUS

Professional business attire is appropriate for this seminar.

Any employee selected to attend this in-service who may be in need of a special accommodation (i.e., sign language

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 07/02/2008

b1
b6
b7C

interpreter; audio loop; personal assistant; large print materials; etc.) should contact [REDACTED]
[REDACTED] as soon as possible.

Any questions concerning this seminar should be directed to the following CITC personnel:

[REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 07/02/2008

b7E

LEAD(s) :

Set Lead 1: (Action)

ALL RECEIVING OFFICES

(U) 1. Division Training Coordinators need to input the attendees' information into the Virtual Academy under the *CI Executive Management Seminar*.

(U) 2. Attendees need to provide via the internal FBI email the following information to SSA [REDACTED] CITC, CD, using the title "*CI Executive Management Seminar*" no later than September 12, 2008:

b6
b7C

- (a) Official Bureau Name and Title
- (b) Name preferred for classroom strip
- (c) SSAN
- (d) Field Office Assignment and telephone number(s) for further contact
- (e) Name and contact information for USIC personnel if you are nominating one for attendance to this course

♦♦

UNCLASSIFIED

~~SECRET~~

FBI Counterintelligence Executive Management Seminar

September 22 – 26, 2008

Monday, September 22nd

8:30am - 8:45am	<i>Welcome to FBI Counterintelligence Training</i> [redacted] [redacted] Supervisory Special Agent [redacted] Supervisory Special Agent Counterintelligence Training Center
8:45am - 9:45am	<i>Counterintelligence Division</i> Stephanie Douglas, Deputy Assistant Director Counterintelligence Division
10:00am - 10:30am	<i>FBI Trends and Initiatives</i> John S. Pistole, Deputy Director
10:30am - 12:30pm	<i>Introduction to Counterintelligence and Legal Authorities</i> [redacted] National Security Law Branch
12:30pm - 1:30pm	<i>Lunch</i>
1:30pm - 2:15pm	<i>Understanding the Threat</i> Virginia L. Bollinger, Section Chief, Analytical Section
2:30pm - 4:30pm	<i>What to do about the Threat: CD Section Unified Battle Plan</i> Jill Marie Eulitz, Section Chief, Eurasia Section Terrence F. Monahan, Acting Section Chief, Global Section Keith D. Salette, Acting Section Chief, East Asia Section
4:30pm	<i>Wrap-up</i>

b6
b7C
b7E

~~SECRET~~

~~SECRET~~

Tuesday, September 23rd

8:30am - 9:30am ***Counterespionage Issues***
Robert Anderson, Jr., Section Chief, Counterespionage
Section

9:30am - 10:15am ***Confidential Human Source Validation: Vital & Essential***
Douglas S. Riggan, Section Chief
[REDACTED] Section

10:30am - 11:15am ***Cyber Division***
James E. Finch, Assistant Director

11:15am - 12:15pm ***National Security Branch***
Arthur Cummings, Jr, Executive Assistant Director
T. J. Harrington, Assistant Executive Assistant Director

12:15pm - 1:15pm ***Lunch***

1:15pm - 2:45pm ***Domain Initiatives: Engaging in Strategic Partnerships;
Working with the Academic and Business Alliances***
J. Chris Woiwode, Acting Section Chief
CI Strategy and Domain Section

3:00pm - 4:00pm ***Regional Counterintelligence Working Groups: Best Practices***
J. Chris Woiwode, Acting Section Chief
[REDACTED] Section

4:00pm ***Wrap up***

b7E

b7E

~~SECRET~~

~~SECRET~~

Wednesday, September 24th

8:00am - 9:00am

[Redacted]

9:00am - 12:00pm

Value of Sophisticated Operations

Jill Marie Eulitz, Section Chief, Eurasia Section

[Redacted] Supervisory Special Agent,

Counterintelligence Training Center

[Redacted] Special Agent, Tampa Division

Guest Speaker

b6
b7C
b7E

12:00pm - 2:00pm

Lunch

[Redacted]

2:00pm - 3:00pm

Round Table Discussion, Best Practices

Seminar Attendees

(S)

3:00pm - 4:00pm

[Redacted]

4:00pm - 5:30pm

Reception

5:30pm - 7:00pm

(S)

[Redacted]

b1
b7E

7:00pm - 7:45pm

Return travel to hotel via bus

~~SECRET~~

~~SECRET~~

Thursday, September 25th

8:30am - 9:15am ***Office of the Director of National Intelligence***
John J. Hess, Associate Director of National Intelligence
Senior Ranking FBI Detainee to [REDACTED] b7E

9:15am - 10:15am ***Counterterrorism Division***
James McJunkin, Deputy Assistant Director

10:30am - 11:15am ***Weapons of Mass Destruction Directorate: Counterproliferation***
Vahid Majidi, Assistant Director

11:15am - 12:00pm ***Directorate of Intelligence***
Kevin Favreau, Assistant Director

12:00pm - 1:00pm ***Lunch***

1:00pm - 2:00pm ***National Security Agency***
[REDACTED]

2:00pm - 3:00pm [REDACTED] ***Resources***
Peter Georgacopoulos, Section Chief
Operations Support to the IC, Surveillance, and Training
Section
[REDACTED] Program Manager
Counterintelligence Training Center

3:00pm - 4:00pm ***Closing Remarks***
Daniel Lee Cloyd, Assistant Director
Richard DesLauriers, Deputy Assistant Director
Counterintelligence Division

4:00pm ***Wrap up***

b6
b7C
b7E

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

DATE: 01-09-2012

CLASSIFIED BY 65179 DMH/STW

REASON: 1.4 (C)

DECLASSIFY ON: 01-09-2037

September 22-25, 2008

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Monday, September 22nd

8:30am - 8:45am

Welcome to FBI Counterintelligence Training

Scott C. Williams, Unit Chief

[redacted] Supervisory Special Agent
[redacted] Supervisory Special Agent
Counterintelligence Training Center

b6
b7C

8:45am - 9:45am

Counterintelligence Division

Stephanie Douglas, Deputy Assistant Director
Counterintelligence Division

10:00am - 10:30am

FBI Trends and Initiatives

John S. Pistole, Deputy Director

10:30am - 12:30pm

Introduction to Counterintelligence and Legal Authorities

[redacted]

b6
b7C
b7E

12:30pm - 1:30pm

Lunch

1:30pm - 2:15pm

Understanding the Threat

Virginia L. Bollinger, Section Chief, Analytical Section

2:30pm - 4:30pm

What to do about the Threat: CD Section Unified Battle Plan

Jill Marie Eulitz, Section Chief, Eurasia Section

[redacted] Global Section
Keith D. Salette, Acting Section Chief, East Asia Section

b6
b7C

4:30pm

Wrap-up

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

September 22-25, 2008

Tuesday, September 23rd

8:30am - 9:30am ***Counterespionage Issues***
Robert Anderson, Jr., Section Chief, Counterespionage Section

9:30am - 10:15am ***Confidential Human Source Validation: Vital & Essential***
Dolores Gilbert, Acting Section Chief
[Redacted] Section

10:30am - 12:00pm [Redacted]
(S) [Redacted] to FBI

b1
b6
b7C
b7E

12:00pm - 1:15pm ***Lunch***

1:15pm - 2:45pm ***Domain Initiatives: Engaging in Strategic Partnerships;
Working with the Academic and Business Alliances***
[Redacted] Section

3:00pm - 4:00pm ***Regional Counterintelligence Working Groups: Best Practices***
[Redacted] Section

b6
b7C
b7E

4:00pm ***Wrap up***

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

September 22-25, 2008

Wednesday, September 24th

8:00am - 9:00am

b6
b7C
b7E

9:00am - 12:00pm

Value of Sophisticated Operations

Jill Marie Eulitz, Section Chief, Eurasia Section

Supervisory Special Agent,

Counterintelligence Training Center

Special Agent, Tampa Division

Guest Speaker

12:00pm - 2:00pm

Lunch

b7E

2:00pm - 3:00pm

Round Table Discussion, Best Practices

Seminar Attendees

(S) 3:00pm - 4:00pm

b1
b7E

4:00pm - 5:30pm

Reception

5:30pm - 7:00pm

(S)

b1
b7E

7:00pm - 7:45pm

Return travel to hotel via bus

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

September 22-25, 2008

Thursday, September 25th

- 8:30am - 9:15am *Office of the Director of National Intelligence*
John J. Hess, Associate Director of National Intelligence
Senior Ranking FBI Detailee to [redacted] b7E
- 9:15am - 10:15am *Counterterrorism Division*
James McJunkin, Deputy Assistant Director
- 10:30am - 11:15am *Weapons of Mass Destruction Directorate: Counterproliferation*
Vahid Majidi, Assistant Director
- 11:15am - 12:00pm *Directorate of Intelligence*
Kevin Favreau, Assistant Director
- 12:00pm - 1:00pm *Lunch*
- 1:00pm - 2:00pm *Cyber Division*
Shawn Henry, Assistant Director
- 2:00pm - 3:00pm [redacted] *Resources*
Peter Georgacopoulos, Section Chief
Operations Support to the IC, Surveillance, and Training Section
[redacted]
Counterintelligence Training Center b6
b7C
b7E
- 3:00pm - 4:00pm *Closing Remarks*
Daniel Lee Cloyd, Assistant Director
Richard DesLauriers, Deputy Assistant Director
Counterintelligence Division
- 4:00pm *Wrap up*

~~SECRET~~

DATE: 12-07-2011
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 12-07-2036

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET//NOFORN~~

Counterintelligence Division

~~SECRET//NOFORN~~

(S)

b1
b7E

(S)

(S)

CI Threat by Country Subprogram Priority

~~SECRET//NOFORN~~

b1
b7E

(S)

Country List for

(S)

Country List for

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

Global Section Countries
Most Likely to Engage in

~~SECRET//NOFORN~~

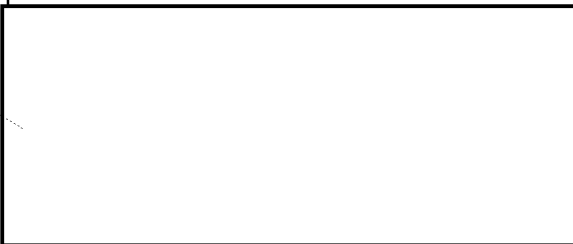
(S)



b1
b6
b7C
b7E

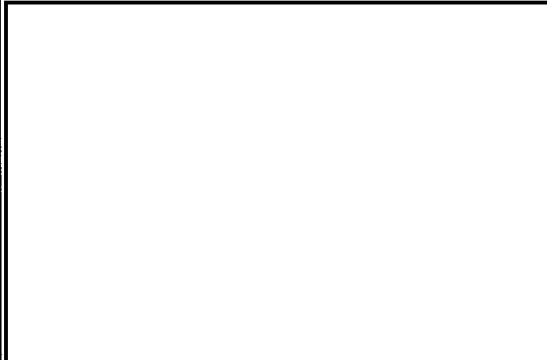
(S)

CI Investigations and
Operations by Section



~~SECRET//NOFORN~~ Current as of 7 May 2008

Global Section Contact Info



b1
b6
b7C

~~SECRET~~

~~SECRET~~

DECLASSIFIED BY 65179 DMH/STW
ON 12-06-2011

The Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM)

Office of the General Counsel
Updated 6/02/08 based on 5/12/08
final draft
This presentation is
UNCLASSIFIED/FOR OFFICIAL USE
ONLY

1

Implementation

- AG signed on _____?
- Effective 1 October 2008?
- Unclassified; markers for provisions in classified Guidelines supplement
- Implementing FBI policy manual will be effective same date as Guidelines
- Entire MIOG and NFIPM being replaced with new CPO policies -- during 2008/2009

FOR OFFICIAL USE ONLY

2

Highlights

- Generally uniform rules for criminal, national security, and foreign intelligence collection cases
- Broader authorities in "assessments" (threat assessments/leads checking)
- Reduced reporting requirements

FOR OFFICIAL USE ONLY

3

Highlights (con't)

- Expanded authorities for investigative assistance and joint operational support to federal, state, local, tribal, and foreign agencies (Part III)
- Express recognition of and authorities for FBI's:
 - Special Events missions
 - Intelligence Analysis and Planning missions (Domain Management)

FOR OFFICIAL USE ONLY

4

Overarching Principle - Respect for Civil Liberties (Introduction, 2nd paragraph)

- "Investigations and other activities must be carried out in a lawful and reasonable manner that **respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding citizens** [and thus] provide the American people a firm assurance that the FBI is acting properly under the law."

FOR OFFICIAL USE ONLY

5

Scope (Part I.A)

- AGG-DOM apply to FBI investigative activities conducted:
 - Within the "United States" (see VII.T - means all areas under territorial sovereignty of the US); or
 - Outside the territories of all countries

FOR OFFICIAL USE ONLY

6

~~SECRET~~

Five AG Guidelines Repealed by AGG-DOM (Part I.D.1)

- (1) General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (2002)
- (2) National Security Investigations and Foreign Intelligence Collection (2003)
- (3) Collection, Retention, and Dissemination of Foreign Intelligence (2006)

FOR OFFICIAL USE ONLY

7

Five AG Guidelines Repealed by AGG-DOM (Part I.D.1) (con't)

- (4) Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Intelligence, Counterintelligence, or International Terrorism Intelligence Investigations (1988)
- (5) Reporting on Civil Disorders and Demonstrations involving a Federal Interest (1976)

FOR OFFICIAL USE ONLY

8

Four General Authorities- FBI is Authorized to: (Part I.B)

- **Conduct investigations** (criminal and national security) and collect foreign intelligence (Part II)
- **Provide investigative assistance** to federal, state, local, tribal, and foreign agencies (Part III)
- **Conduct intelligence analysis & planning** (Part IV)
- **Retain and share information** (Part VI)

FOR OFFICIAL USE ONLY

9

General Principles - Protect US and its People (Part I.C.1)

- **FBI shall fully utilize its authorities** under AGG-DOM to protect the United States and its people from **crimes** in violation of federal law and **"threats to the national security,"** and to further the **foreign intelligence** objectives of the US

FOR OFFICIAL USE ONLY

10

Definition: "Threat to the National Security" (Part VII.S)

- **"International terrorism"** (see VII.J)
- **Espionage and other "intelligence activities"** (see VII.I), sabotage, and assassination, conducted by, "for, or on behalf of "foreign powers"" (see VII.C and G), organizations, or persons;
- **"Foreign computer intrusion"** (see VII.D); and
- AG determined matters per EO 12333

FOR OFFICIAL USE ONLY

11

General Principles - Choice of Methods (Part I.C.2)

- **Least intrusive investigative method feasible will be used, considering the effect on privacy/civil liberties of individuals and potential damage to reputation**
- Choice of methods is a **matter of judgment**
- **FBI shall not hesitate to use any lawful method** consistent with AGG-DOM, where the degree of intrusiveness is warranted in light of seriousness of the matter concerned - **particularly concerning terrorism (balancing test)**

FOR OFFICIAL USE ONLY

12

General Principles – Respect for Legal Rights (Part I.C.3)

- FBI cannot investigate or maintain information on U.S. persons solely for the purpose of monitoring First Amendment activities or the lawful exercise of other Constitutional or legal rights
- **All FBI activities** under AGG-DOM **must have a valid purpose** and be consistent with Constitution, laws, EOs, and DOJ/FBI policies

FOR OFFICIAL USE ONLY

13

Levels of Investigative Activity (Part II)

- **Assessments**
- Predicated Investigations:
 - (1) **Preliminary Investigations**
 - (2) **Full Investigations**
 - Enterprise Investigations

FOR OFFICIAL USE ONLY

14

Assessments; Preliminary and Full Investigations – Common Purposes (Parts II.A.1 and II.B.1)

May be carried out to **detect, obtain information about, or "prevent or protect against"** [includes Special Events Management]:

- Federal crimes
- "Threats to the national security" or
- To collect "foreign intelligence" (see VII.E)

FOR OFFICIAL USE ONLY

15

Assessments - Authorized Activities (Part II.A.3)

- Unlike preliminary or full investigations, there is no required "**predication**" for conducting an assessment
- Instead, an assessment may be conducted for an authorized "**purpose**" [previous slide] if the assessment addresses 1 of 4 assessment "**authorized activities**" [next 3 slides]

FOR OFFICIAL USE ONLY

16

Assessments - Four Authorized Activities (Part II.A.3.a)

Assessment activities that may be carried out for an authorized "purpose" include:

- (1) **Seeking information, proactively or in response to investigative leads,** relating to:
 - activities constituting violations of federal criminal laws or "threats to the national security"
 - the involvement or role of individuals, groups, or organizations in such activities; OR
 - matters of foreign intelligence interest

FOR OFFICIAL USE ONLY

17

Assessments - Four Authorized Activities (Part II.A.3.b and d) (con't)

Assessment activities that may be carried out for an authorized "purpose" include:

- (2) **Identifying and obtaining information about potential targets of or vulnerabilities to** criminal activities in violation of federal law or "threats to the national security"
- (3) **Obtaining information to inform or facilitate intelligence analysis and planning** (Part IV) (includes "Special Events Management" – see VII.Q)

FOR OFFICIAL USE ONLY

18

Assessments - Four Authorized Activities (Part II.A.3.c) (con't)

Assessment activities that may be carried out for an authorized "purpose" include:

- (4) Seeking information to **identify, assess the suitability, credibility, or value of, validate, or maintain the cover or credibility of "human sources"** (see VII.H) who may be able to provide or obtain information relating to criminal activities in violation of federal law, "threats to the national security," or matters of foreign intelligence interest

FOR OFFICIAL USE ONLY

19

Assessments – Eight Authorized Investigative Methods (Parts II.A.4.a and VII.L)

- (1) Obtain "**publicly available**" information
- New definition – deletes "could lawfully be seen or heard by any casual observer"
- Adds "or is obtained by other observation that is not subject to Part V.A.11-12" [ELSUR and physical searches]
- Now includes **physical, video, and photographic (PVP) surveillance** (PVP surveillance is not specifically mentioned anywhere in AGG-DOM)

FOR OFFICIAL USE ONLY

20

New Definition – Publicly Available (Parts II.A.4 and VII.L)

Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, is made available at a meeting open to the public, is obtained by visiting any place or attending any event that is open to the public, or is obtained by other observation or surveillance that is not subject to Part V.A.11-12 [ELSUR or physical searches]

FOR OFFICIAL USE ONLY

21

Assessments – Eight Authorized Investigative Methods (Part II.A.4.b. and c) (con't)

- (2) Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel
- (3) Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies (underlined is new)

FOR OFFICIAL USE ONLY

22

Assessments – Eight Authorized Investigative Methods (Parts II.A.4.d and e and VII.V) (con't)

- (4) Use online services and resources (whether nonprofit or commercial)
- (5) **"Use" and recruit human sources** in conformity with AGG Regarding the Use of FBI Confidential Human Sources (effective 06/13/2007)
 - "Use" means obtaining information from, tasking, or otherwise operating such sources

FOR OFFICIAL USE ONLY

23

Assessments – Eight Authorized Investigative Methods (Part II.A.4.f) (con't)

- (6) Interview or request information from members of the public and private entities
- deletes NSIG restriction = "other than pretext interviews or requests"
- AGG-DOM do not restrict interviews of **potential subjects** – had to have PI under NSIG/Criminal AGG
- AGG-DOM do not mention "pretext" or subject interviews

FOR OFFICIAL USE ONLY

24

Assessments – Eight Authorized Investigative Methods

(Part II.A.4.g and h) (con't)

- (7) Accept information voluntarily provided by governmental or private entities
- (8) Engage in observation or surveillance not requiring a court order

FOR OFFICIAL USE ONLY

25

Predicated Investigations – Approval to Open (Part II.B.2)

- Initiation of a **preliminary or full** investigation requires **supervisory approval** at a level or levels specified in FBI policy (to be determined)
- An **full investigation** to collect **foreign intelligence** must be approved by a SAC or by an FBIHQ official as provided in FBI policy
- “**SAC**” includes Acting SAC, ADIC, or Director designated FBIHQ officials (VII.P)

FOR OFFICIAL USE ONLY

26

Predicated Investigations – Predication to Open

(Part II.B.4)

- **Preliminary:** may be initiated on the basis of **information or an allegation** indicating the existence of 1 of 2 “circumstances”
- **Full:** may be initiated if there is an **articulable factual basis** for the investigation that **reasonably indicates** that 1 of 2 “circumstances” exist

FOR OFFICIAL USE ONLY

27

Predicated Investigations – Circumstances Warranting Investigation (Part II.B.3.a) (PI/Full)

- (1) An activity constituting a federal crime or a “threat to national security” **has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information** relating to the activity or the involvement or role of an individual, group, or organization in such activity

FOR OFFICIAL USE ONLY

28

Predicated Investigations – Circumstances Warranting Investigation (Part II.B.3.b) (PI/Full)

- (2) An individual, group, organization, entity, information, property, or activity **is or may be a target of attack, victimization, acquisition, infiltration, or recruitment** in connection with criminal activity in violation of federal law or a “threat to national security” **and the investigation may obtain information** that would help to **protect against** such activity or threat

FOR OFFICIAL USE ONLY

29

Predicated Investigations – Circumstance Warranting Foreign Intelligence Collection (Parts II.B.3.c & 4.b.i) (Full only)

- The only “**predication**” for a full foreign intelligence investigation is that “**the investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement**”
- No “articulable basis . . . that reasonably indicates” analysis required
- **Full investigations only; no preliminary foreign intelligence investigations (II.B.4)**

FOR OFFICIAL USE ONLY

30

Definition: Foreign Intelligence Requirements (Part VII.F)

- (1) National intelligence requirements issued by DNI, including National Intelligence Priorities Framework; National HUMINT Collection Directives, or successor directives
- (2) Requests to collect foreign intelligence by the President or Intelligence Community officials designated by the President; and
- (3) Directions to collect foreign intelligence by the AG, DAG, or official designated by AG

FOR OFFICIAL USE ONLY

31

Duration of Preliminary Investigations (Part II.B.4.ii)

- Must be concluded within six months of its initiation
- "SAC" may extend up to six months (can NOT delegate to ASAC; but "Acting SAC" is included in SAC definition and can extend)
- Extensions of preliminary investigations beyond one year require FBIHQ approval

FOR OFFICIAL USE ONLY

32

Case Initiation Notice Requirements to DOJ (Part II.B.5)

- **Assessments:** no notice requirements
- **Predicated cases:**
 - Case initiation notice to DOJ required in five instances
 - Notice in each of these instances shall be as soon as possible but NLT 30 days after initiation of the investigation
 - Not much specification of content of notice; FBI policy will describe

FOR OFFICIAL USE ONLY

33

Notice Requirements – Sensitive Investigative Matter (Part II.B.5.a)

- (1) Field office notifies FBIHQ and US Attorney (or other appropriate DOJ official) of a field-initiated preliminary or full investigation involving a "sensitive investigative matter" (FBIHQ gives same notice for HQ-initiated cases)
 - DOJ NSD must also be notified if the investigation concerns a "threat to the national security"
 - All notices shall identify all sensitive matters involved in the investigation

FOR OFFICIAL USE ONLY

34

Definition – Sensitive Investigative Matter (Part VII.N)

- "An investigative matter involving a domestic public official, political candidate, religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI HQ and DOJ officials"

FOR OFFICIAL USE ONLY

35

Case Initiation Notices to National Security Division DOJ (Parts II.B.5.b & C.3) (con't)

- FBI shall notify DOJ NSD of the initiation of:
 - (2) Any full investigation of a US person relating to a threat to the national security
 - (3) Any full investigation to obtain foreign intelligence
 - (4) Any preliminary or full espionage investigation
 - (5) Any enterprise investigation (EI)
 - criminal EI cases – notice to Organized Crime and Racketeering Section, DOJ Criminal Division
 - Field must also notify any relevant USAO (except in espionage cases) and FBIHQ of EI cases

FOR OFFICIAL USE ONLY

36

Annual Reports (Part VI.D.1.a)

- From FBI to DOJ NSD concerning FBI **"foreign intelligence collection program"**, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office."
- **All other annual reports eliminated**

FOR OFFICIAL USE ONLY

37

Enterprise Investigations (EI) (Part II.C.1) - Definition

- Full investigation of a **group or organization** may be initiated as an EI if there is an articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provisional support for **1 of 5 listed activities**:

FOR OFFICIAL USE ONLY

38

Enterprise Investigations (EI) (Part II.C.1) - Definition (con't)

- (1) A **pattern of racketeering activity** as defined in 18 USC 1961(5)
- (2) **"International terrorism"** (defined in Part VII.J) or other **"threat to the national security"**
- (3) **Domestic terrorism** as defined in 18 USC 2331(5) involving a violation of federal criminal law

FOR OFFICIAL USE ONLY

39

Enterprise Investigations (Part II.C.1) - Definition (con't)

- (4) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
- (5) An offense described in 18 USC 2332b(g)(5)(B) [**federal crimes of terrorism**] or 18 USC 43 [**force, violence, and threats involving animal enterprises**] [18 USC 43 is new]

FOR OFFICIAL USE ONLY

40

Enterprise Investigations (EI)- Scope (Part II.C.2)

- EI may examine the structure, scope, and nature of group/organization including:
 - Relation to "foreign power," if any
 - Identity/relationships of members/persons who may be acting in furtherance of its objectives
 - Its finances and resources;
 - Its geographical dimensions; and
 - Its past and future activities and goals

FOR OFFICIAL USE ONLY

41

Predicated Investigations - Authorized Investigative Methods Parts II.B.4 and V.A.11-12

- **All lawful methods** may be used, except that ELSUR and physical search warrants (more strict than Criminal AGG) may NOT be used in a **preliminary** investigation
- Some methods have special restrictions, review, or approval requirements
- All 8 methods authorized in an assessment may be used in a predicated investigation

FOR OFFICIAL USE ONLY

42

**Predicated Investigations –
Authorized Investigative Methods -
Include (Parts V.A.2-3 and 6)**

- Mail covers
- Physical searches of personal or real property where **no warrant** or court order is legally required because no reasonable expectation of privacy (e.g. **trash covers**)
- Polygraph examinations

FOR OFFICIAL USE ONLY

43

**Predicated Investigations –
Authorized Investigative Methods – New
Rule: Consensual Monitoring – (Part V.A.4)**

- **"Consensual monitoring"** (see VII.A) of communications, including consensual computer monitoring
 - **Prosecutor clearance no longer required in criminal cases; 2002 AG Consensual Monitoring Guidelines (criminal) no longer apply to FBI**
 - **FBI legal review by CDC or OGC required in all cases now**

FOR OFFICIAL USE ONLY

44

**Predicated Investigations –
Authorized Investigative Methods –
Consensual Monitoring – (Part V.A.4) (Cont)**

- When a **"sensitive monitoring circumstance"** is involved, the monitoring **must be approved by DOJ's Criminal Division** or, if the investigation concerns a "threat to the national security" or foreign intelligence, by DOJ's **National Security Division**

FOR OFFICIAL USE ONLY

45

**Consensual Monitoring – 4 Part
Definition of "Sensitive Monitoring
Circumstance" (Part VII.O)**

- (1) Investigation of member of Congress, federal judge, Executive Branch member at Executive Level II or above, or a person who has served in such capacity within the previous 2 years;
- (2) Investigation **concerning an offense involving bribery, conflict of interest, or extortion related to performance of official duties** of a Governor, LT Gov, or AG of a state/territory or judge/justice of the highest court of state/territory;

FOR OFFICIAL USE ONLY

46

**Consensual Monitoring – 4 Part
Definition of "Sensitive Monitoring
Circumstance" (Part VII.O) (cont)**

- (3) A party to the communication is **in custody** of the **Bureau of Prisons** or the **US Marshal Service** or is being or has been afforded protection in the **Witness Security Program**; or
- (4) The AG, DAG, or an Assistant AG has requested that the FBI obtain prior approval for the use of consensual monitoring in a **specific investigation**

FOR OFFICIAL USE ONLY

47

**Predicated Investigations –
Authorized Investigative
Methods - Include (Part V.A.5)**

- Use of closed-circuit television, direction finders, and other monitoring devices
 - **Prior legal review by CDC or FBI OGC** required to ensure compliance with all applicable legal requirements
 - These methods usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications

FOR OFFICIAL USE ONLY

48

**Predicated Investigations –
Authorized Investigative
Methods - Include (Part V.A.7)**

- **Undercover operations (UC)**
 - In **criminal** investigations, UC must be carried out in conformity with 2002 AGG on FBI Undercover Operations
 - If threats to national security or foreign intelligence involved, UC involving **religious or political organizations** require FBIHQ approval, with DOJ NSD participation in the review process

FOR OFFICIAL USE ONLY

49

**Predicated Investigations –
Authorized Investigative
Methods - Include (Part V.A.8)**

- **Compulsory process authorized by law:**
 - Grand Jury and other subpoenas
 - National Security Letters
 - FISA Business Record orders (50 U.S.C. §§ 1861-63) [for "tangible things"]

FOR OFFICIAL USE ONLY

50

**Predicated Investigations –
Authorized Investigative
Methods - Include (Parts V.A.9-10)**

- Accessing **stored wire and electronic communications and transactional records** (18 U.S.C. §§ 2701-2712)
- Use of **pen registers/trap and trace devices:**
 - 18 U.S.C. §§ 3121-3127 (criminal)
 - 50 U.S.C. §§ 1841-1846 (FISA)

FOR OFFICIAL USE ONLY

51

**Full Investigations Only –
Authorized Investigative
Methods - Include (Parts V.A.11-12)**

- **Electronic surveillance and physical searches** (including mail openings):
 - 18 U.S.C. §§ 2510-2522 and Rule 41, Fed. Rules of Criminal Procedure (criminal)
 - 50 U.S.C. §§ 1801-1811 and 1821-1829 (FISA)
 - Section 2.5, Executive Order 12333 (for intelligence purposes against a foreign power or agent thereof)
 - **Classified limitation on certain searches**

FOR OFFICIAL USE ONLY

52

**Predicated Investigations –
Authorized Investigative Methods –
Special Requirements (Part V.B.1)**

- **Contacts with Represented Persons:**
 - If individual known to be represented by counsel in a particular matter, follow applicable FBI and DOJ procedures in the absence of prior notice to counsel

FOR OFFICIAL USE ONLY

53

**Predicated Investigations – Authorized
Investigative Methods – Otherwise Illegal
Activities (OIA) (Parts V.C and VII.B)**

- OIA rules apply to FBI agents and "employees" (includes employee of another agency working under FBI control/direction)
- **OIA in criminal undercover operation** – follow 2002 AGG "Undercover Operations"
- **OIA by human source** – follow 2006 AGG "Confidential Human Sources"

FOR OFFICIAL USE ONLY

54

Predicated Investigations – Authorized Investigative Methods – Otherwise Illegal Activities (OIA) (Parts V.C and VII.B)

OIA in national security and foreign intelligence cases:

- Complicated 2-page set of rules
- Limited SAC approval authority
- NSD DOJ approval authority for remainder
- Consult with CDC; contact NSLB operational attorneys for assistance

FOR OFFICIAL USE ONLY

55

Assistance to Other Agencies – General (Part III)

- Under Part III, FBI may provide **investigative assistance** to other federal, state, local, tribal, or foreign agencies including **joint operations and activities**
- **Part III does NOT limit FBI's investigative authorities under Part II – III adds additional authorities; may use either Part II or Part III, as appropriate**

FOR OFFICIAL USE ONLY

56

Assistance to US Intelligence Community (Part III.A)

- FBI may provide investigative assistance (**including operational support**) to authorized intelligence activities of other US Intelligence Community agencies

FOR OFFICIAL USE ONLY

57

Assistance to Other Federal Agencies (Part III.B.1)

- FBI may provide assistance to any federal agency in the investigation of
 - Federal crimes
 - Threats to national security
 - Foreign intelligence collection
 - Any other legally authorized purpose (e.g. support of Secret Service protective responsibilities)

FOR OFFICIAL USE ONLY

58

Assistance to State, Local, or Tribal Agencies (Part III.C)

- FBI may provide **investigative assistance** to state, local, or tribal agencies in investigation of **matters that may involve:**
 - Federal crimes;
 - Threats to the national security; or
 - For other legally authorized purposes

FOR OFFICIAL USE ONLY

59

Assistance to Foreign Agencies – (Part III.D.1)

- At the request of foreign law enforcement, intelligence, or security agencies, FBI may **conduct investigations or provide investigative assistance** to investigations by such foreign agencies, **consistent with US interests and with due consideration of the effect on any US person**

FOR OFFICIAL USE ONLY

60

Assistance to Foreign Agencies – (Part III.D.1) (con't)

- Must coordinate/notify ☐ if required by FBI ☐
- FBI shall notify DOJ NSD w/i 30 days of investigation or assistance under prior slide if:
 - (1) FBI implementing policy requires FBIHQ approval for the assistance; AND
 - (2) Assistance relates to a threat to the national security

FOR OFFICIAL USE ONLY

61

Assistance to Foreign Agencies – Agent Notification to AG (Part III.D.2)

- FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the US unless such foreign officers have provided prior notification to the AG (18 USC 951 - Agents of Foreign Governments – does not include diplomatic or consular officer or attache)

FOR OFFICIAL USE ONLY

62

b7E

Assistance to Other Agencies – Applicable Standards and Procedures – General (Part III.E)

- Authorized FBI investigative assistance under Part III includes **joint operations and activities**
- All lawful methods may be used under Part III
- Special rules if using techniques not authorized in assessments

FOR OFFICIAL USE ONLY

63

Assistance to Other Agencies – Applicable Standards and Procedures – Methods not Authorized in Assessments (Part III.E.3)

- Three requirements to use investigative methods not authorized in assessments:
 - (1) Same FBI supervisory approval as would be required for that technique in a predicated investigation
 - (2) If "sensitive investigative matter" involved, must give DOJ same notice as if it were a predicated investigation (Part II.B.5)

FOR OFFICIAL USE ONLY

64

Assistance to Other Agencies – Applicable Standards and Procedures – Methods not Authorized in Assessments (Part III.E.3)

- Three requirements to use investigative methods not authorized in assessments:
 - (3) FBI must maintain database or records system that permits, with respect to each such activity, the prompt retrieval of
 - activity status (open or closed);
 - dates of opening and closing; and
 - basis for the activity

FOR OFFICIAL USE ONLY

65

Intelligence Analysis and Planning – General (Parts IV and II.A.3.d)

- Under Part IV, FBI may draw on all lawful sources of information, data, or intelligence, including but not limited to results of investigative activities under AGG-DOM
- FBI may conduct assessments to obtain information to inform or facilitate Part IV analysis and planning

FOR OFFICIAL USE ONLY

66

Intelligence Analysis and Planning – Strategic Intelligence Analysis (Part IV.A)

- FBI may conduct analysis of:
 - Matters relevant to US **foreign affairs**
 - Threats to and vulnerabilities of the US including domestic and international:
 - **Criminal** threats and activities; and
 - Activities, circumstances, and developments affecting **national security**
 - **Special Events Management**

FOR OFFICIAL USE ONLY

67

Intelligence Analysis and Planning – Strategic Intelligence Analysis (Part IV.A) (con't)

- Analysis may encompass:
 - Present, emergent, and potential **threats and vulnerabilities**;
 - Their **contexts and causes**; and
 - Identification and analysis of **means of responding to them**

FOR OFFICIAL USE ONLY

68

Intelligence Analysis and Planning – Reports and Assessments Generally (Part IV.B)

- FBI may conduct research, analyze info, prepare reports/assessments concerning:
 - Types of criminals or criminal activities;
 - Organized crime groups;
 - Terrorism and other threats to national security;
 - Foreign intelligence matters; or
 - Scope and nature of **criminal activity in particular geographic areas or sectors of the economy**

FOR OFFICIAL USE ONLY

69

Intelligence Analysis and Planning – Intelligence Systems (Part IV.C)

- FBI may **operate intelligence, identification, tracking, and other information systems**:
 - In support of authorized investigative activities, or
 - For such other or additional purposes as may be legally authorized (e.g. intelligence and tracking systems relating to terrorists, gangs, or organized crime groups)

FOR OFFICIAL USE ONLY

70

Retention of Information (Part VI.A)

- (1) FBI shall **retain records** relating to activities under AGG-DOM
- (2) FBI shall maintain a **database/records system** that permits, with respect to **each predicated investigation**, the prompt retrieval of:
 - Status of investigation (open or closed);
 - Dates of opening and closing; and
 - Basis for the investigation

FOR OFFICIAL USE ONLY

71

Permissive Information Sharing – Generally (Part VI.B.1.a)

- **Consistent with law and agreements with other agencies concerning dissemination of information they provided, FBI may disseminate information** obtained or produced under AGG-DOM:
 - (1) Within the FBI and to other DOJ components

FOR OFFICIAL USE ONLY

72

**Permissive Information Sharing –
Generally (Part VI.B.1.b and g)
(con't)**

- (2) To other federal, state, local, or tribal agencies if related to their responsibilities
 - Other IC elements may decide whether info is related to their responsibilities
- (3) If dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. § 552a)

FOR OFFICIAL USE ONLY

73

**Permissive Information Sharing
– Generally (Part VI.B.1.d) (con't)**

- (5) To foreign agencies if three conditions met:
 - Info is related to their responsibilities;
 - Dissemination consistent with US interests; **and**
 - FBI has considered effect dissemination may reasonably be expected to have on any identifiable US person;

FOR OFFICIAL USE ONLY

74

**Permissive Information Sharing –
Generally (Part VI.B.1.e-f) (con't)**

- (6) If information is publicly available, does not identify US person, or is disseminated with the consent of the person to whom it concerns
- (7) If dissemination is necessary to **protect the safety or security** of persons or property, to protect against or prevent a crime or threat to national security, or to obtain information for the conduct of an authorized FBI investigation

FOR OFFICIAL USE ONLY

75

**Required Information
Sharing – (Part VI.B.2)**

- **FBI shall share and disseminate information** as required by all statutes, treaties, Executive orders, Presidential directives, National Security and Homeland Security Council directives, policies, and AG-approved policies and MOUs/MOAs

FOR OFFICIAL USE ONLY

76

**Information Related to Criminal Matters
– Coordination with Prosecutors (Part VI.C.1)**

- In investigation relating to **possible criminal activity** in violation of federal law, **case agent shall maintain** periodic written or oral **contact with the appropriate federal prosecutor**, as circumstances warrant or as requested by the prosecutor.

FOR OFFICIAL USE ONLY

77

**Information Related to Criminal
Matters Outside FBI Jurisdiction
(Part VI.C.2)**

- **Field office shall promptly refer** credible info concerning serious criminal activity to LE agency having jurisdiction **unless** disclosure would jeopardize ongoing investigation, endanger safety of an individual, disclose identity of human source, interfere with a source's cooperation, or reveal legally privileged information
- **If no full disclosure within 180 days**, field office must notify FBIHQ in writing of facts and circumstances; HQ notifies **DAG**

FOR OFFICIAL USE ONLY

78

Information Related to **Criminal Matters**
– **Reporting FBI Personnel for Criminal Activity** (Part VI.C.3)

- When it appears that an **FBI agent or "employee"** (see VII.B) has engaged in criminal activity during an investigation – **notify US Attorney's office or an appropriate DOJ Division** (If **human source** – proceed under AG Human Source Guidelines)
- Approved **Otherwise Illegal Activities or minor traffic offenses** are excepted from reporting requirement

FOR OFFICIAL USE ONLY

79

National Security and Foreign Intelligence Information Sharing –
General Rules (Part VI.D)

- **Responsibility to provide** information to agencies with relevant responsibilities to protect US from terrorism, **except as limited by specific constraints on such sharing**
- **Dissemination of FISA info** – AG approval required for use in criminal (includes administrative) proceeding
- **NSL statutes** – some statutory restrictions
- **Human source identity** disclosure governed by AG Human Source Guidelines

FOR OFFICIAL USE ONLY

80

National Security and Foreign Intelligence Information Sharing – **DOJ – US Attorney Offices** (Part VI.D.1.c-e)

- **Designated personnel** (with clearances and training) in relevant US Attorney Offices shall have access to and receive information from FBI concerning national security and FI
 - **Espionage cases:** NSD must authorize US Attorney Office access (NSD has 60 days to decide after FBI notifies NSD of espionage case)
 - If NSD authorizes, access in US Attorney Office is limited to designated personnel

FOR OFFICIAL USE ONLY

81

Questions ???

- Chief Division Counsel
- OGC, National Security Law Branch (national security and foreign intelligence cases)
- OGC, Investigative Law Unit (criminal cases)

FOR OFFICIAL USE ONLY

82

~~SECRET~~

~~SECRET~~

DECLASSIFIED BY 65179 DMH/STW
ON 12-07-2011

STANDARD FBI MINIMIZATION PROCEDURES

(Revised 2008)

ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH

9/4/05 version

~~SECRET~~

1

BACKGROUND

UNCLASSIFIED

2

- Foreign Intelligence Surveillance Act (1978)
- Statute imposes requirements to properly handle acquisition, retention & dissemination of non-publicly available U.S. Person information
- Failure to follow Minimization Procedures is a violation of the statute and court order

UNCLASSIFIED

3

- Standard Minimization Procedures are approved by the Attorney General
- Filed with the Foreign Intelligence Surveillance Court (FISC)
- Incorporated into every order issued by the FISC

UNCLASSIFIED

4

- 2008 Standard Minimization Procedures (SMP's) will replace multiple sets of procedures that have been in effect since 1997
- Anticipated date of implementation of 2008 SMP's is November 1, 2008

~~SECRET~~

5

- One set of procedures for FBI
- Incorporates use of electronic databases
 - New access policies
- Incorporates importance of sharing FISA information
- Transition period

~~SECRET~~

6

~~SECRET~~

~~SECRET~~

ACLURM041996

OVERVIEW

UNCLASSIFIED

7

KEY DIFFERENCES

OLD	NEW
Logging & indexing	No Longer Needed
Indefinite Retention	Specific Time Limits
2 Categories of privileged communications	3 Categories
Known & extended absence rule	Eliminated
Limited Dissemination	More expansive, especially to Foreign Governments

~~SECRET~~

8

Key Definitions

- The "Standard" (from SMP)
- U.S. person (from FISA)
- Foreign Intelligence (from FISA)
- Marking (from SMP)
- "Raw" FISA Information (from SMP)

~~SECRET~~

9

The "STANDARD"

reasonably appears

- to be foreign intelligence information,
 - to be necessary to understand foreign intelligence information or to assess its importance,
- OR
- to be evidence of a crime

~~SECRET~~

10

U.S. PERSON

- US Citizen
- Permanent Resident Aliens
- US Corporations
- A group substantially composed of US Persons
- Presumptions
 - Known US or unknown location - USP
 - Known outside US - Non-USP
 - Online operation w/no further info - Non-USP

~~SECRET~~

11

Foreign Intelligence

- Information that relates to, and if concerning a USP is necessary to, the ability of the US to protect against
 - actual or potential attack or other grave hostile acts of FP/agents or sabotage, international terrorism, or the international proliferation of weapons of mass destruction by FP/agents; or
 - clandestine intelligence activities by an intelligence service or network of FP or by an agent of FP
- OR
- Information with respect to a foreign power or foreign territory that relates to, and if concerning a USP is necessary to,
 - National defense or security of US; or
 - Conduct of US foreign affairs

UNCLASSIFIED

12

"RAW Information"

FISA-acquired info that:

- Is in the same or substantially same format as when FBI acquired it, or
- Has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it meets the standard

AND

- Has not been evaluated to determine whether it meets the standard.

~~SECRET~~

13

Marking

A designation given to FISA information, generally in an electronic and data storage system such as [REDACTED] indicating that:

- a determination has been made that raw FISA-acquired information meets certain criteria set out in the SMP; or
- that something further needs to be done with the information from a workflow perspective

UNCLASSIFIED

14

b7E

ACQUISITION

Immediately after the court order is signed we are in the ACQUISITION phase

UNCLASSIFIED

15

Acquisition - General

- NSD attorney shall conduct a minimization briefing following the authorization of the FISA
- FBI verify facility before initiating
 - Continuing obligation to verify target uses or is about to use
- Must be pursuant to means and extent approved in the court order
- Know the Standard Techniques

~~SECRET~~

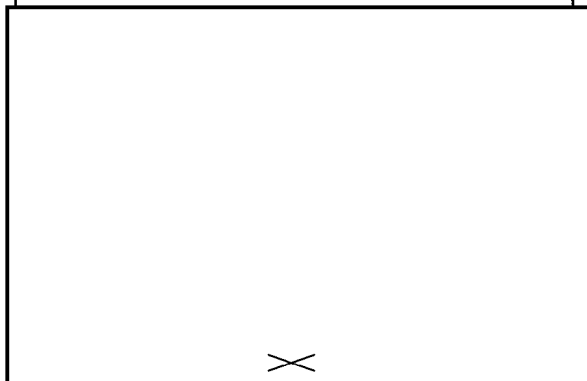
16

Acquisition - Elsur



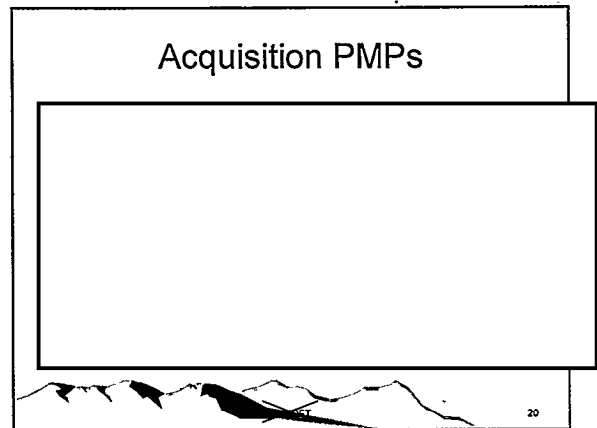
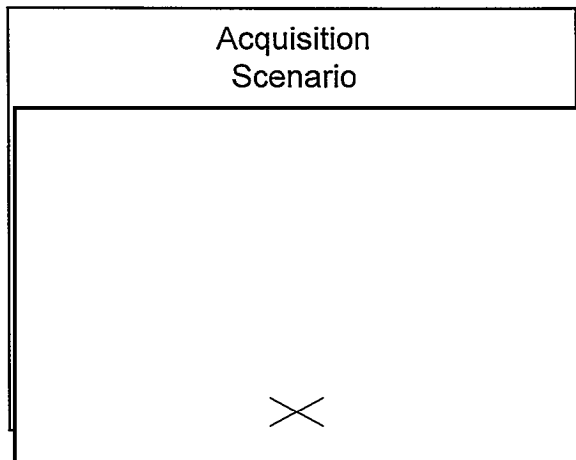
17

Acquisition Scenario

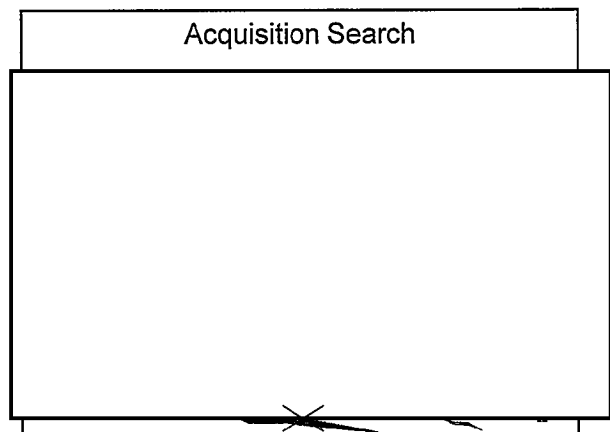
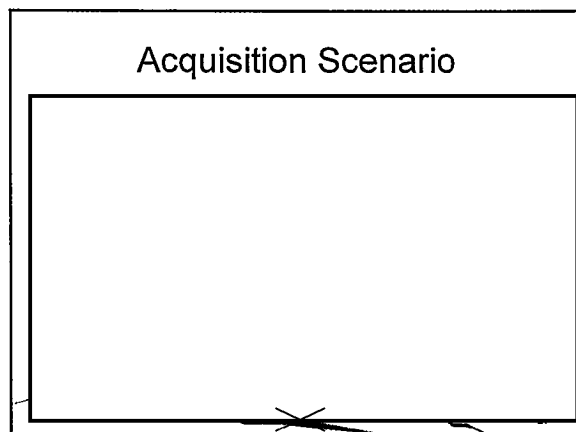


~~SECRET~~

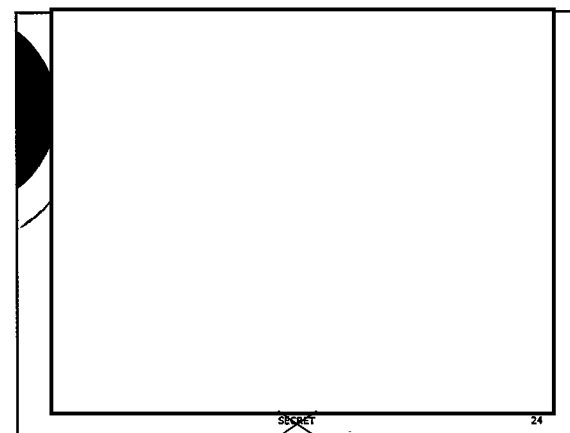
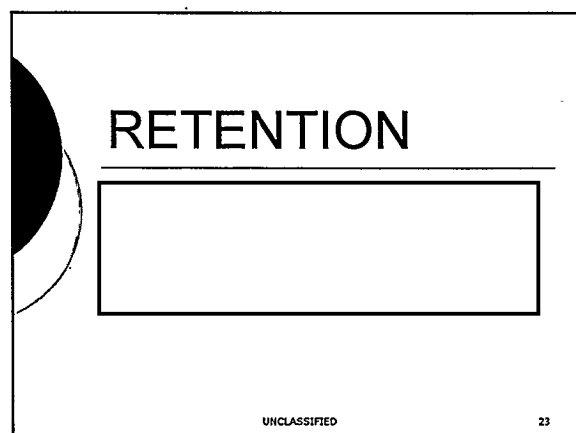
b7E



b7E



b7E



b7E

Review of Raw FISA-acquired Info

- o "Authorized personnel" may review, translate, copy, summarize, analyze, and use raw FISA-acquired information only as necessary to evaluate whether it meets the "standard"
- o "AUTHORIZED PERSONNEL" = all employees, contractors & others authorized to work under the direction & control of the FBI on FISA related matters. Does not include other government employees.

~~SECRET~~

25

Marking

- o New SMP and new FBI access policy contemplate wider access to raw FISA information
- o Concept of Case Coordinators Established: Case coordinators will be the agent with primary responsibility for the FISA and his/her designees
- o Although other authorized users can access data
 - ONLY a case coordinator may mark the information within the systems for minimization purposes
 - Other authorized users can request that a case coordinator mark information
 - o There must be a written record of the name of the requester, the date the marking was authorized, and the case file number to which the marking relates
- o Disputes regarding marking resolved pursuant to FBI policy

~~SECRET~~

26

Markings

- o Reasonably appears to be foreign intelligence information
- o Necessary to understand foreign intelligence information or assess its importance
- o Evidence of a crime

Cont'd.....

~~SECRET~~

27

Markings

- o Privileged and target charged with a crime pursuant to the U.S. code
- o Privileged and target charged with a non-federal crime or non-target charged with a crime in the U.S.
- o Other privileged communications involving targets or others not charged with a crime in the U.S.
- o Potentially privileged

Cont'd.....

~~SECRET~~

28

Markings

- o For Prosecutorial Review (i.e., if you think it falls under Brady, Jencks, Rule 16, etc.)
- o Non-pertinent communication
- o Sensitive communication (falls within established non pertinent category)
- o Does not meet 3rd party standard

~~SECRET~~

29

Retention - Marking Transition

- o
 - New markings
 - o take acquired after date of new procedures
 - o old unreviewed take
 - Old markings
 - o reviewed and marked old take (i.e., pertinent/non-pertinent)
 - o don't have to go back and re-mark if already marked under the old SMPs
- o Other systems will not have these new markings

~~SECRET~~

30

b7E

Retention - Time Limits

Retention of data in electronic data & storage systems (outside of systems will be controlled by AG Guidelines and NARA)

- o Unreviewed Raw info destroyed after 5 years
- o Reviewed and does NOT meet the "standard"
 - Access limited after 10 years
 - Information destroyed after 15 years

~~SECRET~~

31

Retention - Time Limits

- o Meets the "standard"

- No retention time limit (NARA still applies)
- Before using FBI shall strike, or substitute a characterization for, information of or concerning a USP, including a USP identity, if it does not meet the standard
- Evidence of a crime but not FI may be retained and disseminated for law enforcement purposes only

~~SECRET~~

32

Retention Scenario

- o Case agent marks USP communication as non-pertinent
- o Analyst or agent from another field office searching for FI related to their investigation thinks information marked non-pertinent reasonably appears to be FI
- o What do they need to do to mark the communication?
- o What if analyst/agent from other field office wants to put the information in an EC or IIR?

~~SECRET~~

33

Categories of Non-Pertinent Communications

- o FBI case agent should continually analyze to establish categories of information that do not generally meet the standard
 - Establish after a reasonable period of monitoring
 - Report to FISC in renewal
 - Specific to each FISA
- o When developing categories consider the follow types of sensitive information: Religious activities, educational and academic activities, political activities, sexual or highly personal activities, medical or psychiatric activities, matters involving minor children

~~SECRET~~

34

THIRD PARTY OVERHEARS OLD NEW

- | | |
|---|---|
| <ul style="list-style-type: none"> o Info about US persons can only be retained if the information was about the target or his activities o Not on a known or extended absence of a US person | <ul style="list-style-type: none"> • KEEP AND USE IF: <ul style="list-style-type: none"> • Is a communication made or received on behalf of the target, <u>or</u> • Concerns activities in which the target is or may be involved, <u>or</u> • Concerns a serious threat of injury, loss of life, damage to property, or damage to the national security • KEEP BUT CANNOT USE IF <ul style="list-style-type: none"> • Meets the "standard" but does not meet the rules above |
|---|---|

~~SECRET~~

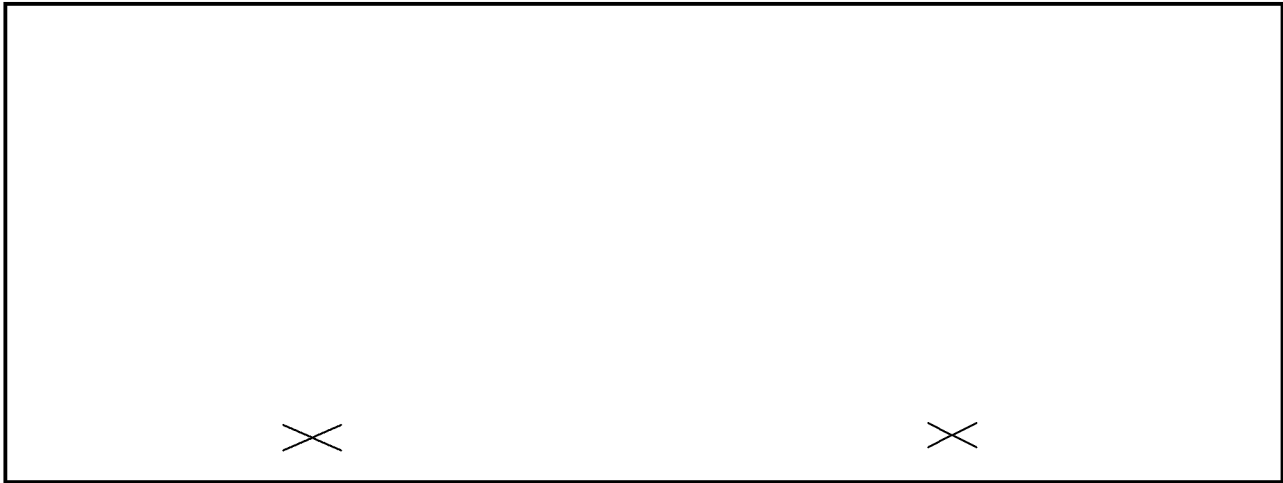
35

Privileged Communications

- o Category 1
 - Target is charged with Federal Crime
- o Category 2
 - Target is charged with non-federal crime in US or Non-Target charged with any crime in US
- o Category 3
 - Communications between attorneys and targets/others not charged with a crime in the US

~~SECRET~~

36



Sharing FISA Information with Prosecutors

- o Can get access to RAW FISA Information
 - Trained on minimization procedures
 - Need to know (EO 12333)
- o Can get access to RAW FISA Information directly from FBI databases with
 - Proper Request pursuant to new FBI and AG policy
 - o With FBIHQ Approval (AD and OGC)
 - Comply with procedures for database access
- o Doesn't change prosecutor's ability to satisfy "criminal discovery obligations"

~~SECRET~~

39

Sharing FISA Information with Prosecutors

- o In coordination with FBIHQ and NSLB, prosecutors may disclose FISA-acquired information to witnesses, targets or subjects of an investigation, or their respective counsel
 - except that prosecutors may not disclose FISA-acquired information which could not be FI or is not evidence of a crime
- o Does not change obligation to comply with other legal requirements such as rules regarding classification and use authority

~~SECRET~~

40

Retention - Queries

- o SMPs specifically contemplate querying raw FISA-acquired information to find information that would meet the standard
- o Queries should be designed to find and extract FI, evidence of a crime, or Brady
- o Records will be kept of all queries
- o Queries may be subject to review

~~SECRET~~

41

[DISSEMINATION]

As soon as information is shared, we are in the DISSEMINATION phase

UNCLASSIFIED//FOUO

42

Dissemination

- General rule: can only disseminate FISA information that meets the "standard"
 - FI may be disseminated to federal, state, local, and tribal officials and agencies
 - USP identities shall not be disseminated unless necessary to understand the FI or to assess its importance

~~SECRET~~

43

Dissemination

- If disseminating FISA information that meets the "standard," a user must indicate within the system, when and in what form the dissemination was made
- Users other than the case coordinators must notify the case coordinator at least 5 days prior to disseminating FISA information.
- In emergency situations, where dissemination is required immediately to prevent a threat to human life, notification should occur within 48 hours after dissemination

~~SECRET~~

44

Dissemination - Technical or Linguistic Assistance

- SMPs incorporate technical and linguistic assistance procedures
 - No need to repeat this language in the FISA application and order under new SMP
 - Restrictions on use by other federal agencies
 - May not keep permanent records of such raw FISA-acquired information
 - Must destroy or return raw FISA-acquired information to FBI at the conclusion of their assistance
- Applies retroactively

~~SECRET~~

46

b7D
b7E

Dissemination of Raw Take in Terrorism Cases

- SMP incorporates the raw take order from FISC
 - No need to discuss in FISA applications or orders anymore
 - Can only disseminate the raw FISA-information in cases covered by the raw take order and its successor orders
 - No court order to go by
 - Need to determine based on the type of case whether can make this dissemination.
- Applies retroactively

~~SECRET~~

47

Emergency Situations

- **To protect national security, enforce criminal law, or protect life or property from serious harm, immediately**
 - Notify FBI HQ and NSD
 - Request that NSD obtain a modification
 - Such modification needs to be approved by the AG and presented to the FISC
- **To protect against an "immediate threat to human life"**
 - Notify NSD promptly and NSD shall promptly notify the FISC

~~SECRET~~

48

Oversight by DOJ-NSD

- Periodic minimization reviews mandated
 - Access to all FISA information for these reviews
 - Review ECs or other documents containing FISA information that has been uploaded/disseminated
 - Review FBI systems containing raw information
 - Audits of queries
 - Audits of access to FBI systems

UNCLASSIFIED

49

Questions???

- NSLB
- NSD/OI

UNCLASSIFIED

50

~~SECRET~~

DATE: 01-10-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DISCOVERY REQUEST MATERIAL

COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR

DECEMBER 1-4, 2008

~~SECRET~~

Counterintelligence Training Center						7/13/2011	
Please complete this form to [] to [] TR # []							
Class Name:	CI Executive Management Seminar 08-01					Virtual Academy: yes or no	
Travel Dates:	11/30/2008					* required information -	
Class Dates:	12/1-4/2008						
Class Location:	SIOC						
Class Coordinator:				Section/Unit Sponsor:			
Notes:							
*	*		*	*	*		
Last Name	First Name	MI	Title	SSN	FO	Telephone	Notes
							Secretary

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-06-2011 BY 65179 DMH/STW

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 11/21/2008

Date: 10/27/2008

To: All Field Offices

Attn: SACs
ASACs
Training Coordinators

From: Counterintelligence

Counterintelligence Training Center, [REDACTED]

Contact: SSA [REDACTED]
[REDACTED]

b6
b7C
b7E

Approved By: [REDACTED]

Drafted By:

Case ID #: [REDACTED] (Pending)

Title: COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR;
COUNTERINTELLIGENCE DIVISION;
COUNTERINTELLIGENCE TRAINING CENTER (CITC);
DECEMBER 1 - 4, 2008;
FBIHQ, STRATEGIC INFORMATION AND OPERATIONS CENTER

Synopsis: To advise receiving offices of captioned seminar and to provide administrative information.

Details: The Federal Bureau of Investigation (FBI) National Strategy for Counterintelligence (CI) mandates an increased focus on both the professionalization of the FBI CI workforce, and the training required to establish that professionalized cadre. As part of this training, the Counterintelligence Division (CD) has developed and mandated a CI Executive Management Seminar for all Special Agents-in-Charge (SACs) and Assistant Special Agents-in-Charge (ASACs) who are overseeing CI operations, have not already attended this seminar, and are not considered proficient in CI. The seminar will focus on various topics outlined in the National Strategy for CI.

CI proficiency for Executive Managers is defined as three (3) years in the CI program and two (2) CI courses of any

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 10/27/2008

b7E

kind, either FBI or United States Intelligence Community (USIC) sponsored.

While the seminar is open to all field executives, preference will go to those executives assigned to the CI program. The seminar is being held at the Strategic Information and Operations Center (SIOC). Space is limited to 30 seats.

In an effort to foster continuing collaboration with our USIC partners, CITC has opened this seminar to the USIC. CITC will be working with the training divisions of each USIC agency to identify attendees from the USIC. However, if you are attending this course and would like to nominate an equivalent executive (GS-15/SES) from the USIC, please forward the name to CITC with your registration information. This is only a nomination. Final selection will be made by the CD through liaison with the USIC agency's training office. While the FBI will cover materials and course fees for the USIC attendees, the travel and per diem costs must be incurred by the individual agencies.

COURSE LOCATION AND DURATION

The CI Executive Management Seminar will be held in the [REDACTED] FBIHQ. The seminar will start promptly at 8:30 AM on Monday, December 1, 2008 and will end at approximately 5:00 PM on Thursday, December 4, 2008.

b7E

Sunday, November 30, 2008 is the designated travel day for this seminar. If possible, no travel arrangements should be made with a departure time prior to 6:00 PM, Thursday, December 4, 2008.

On Tuesday, December 2, 2008, there will be an evening event at the [REDACTED]. Transportation to and from this event will be provided. As food will be provided, per diem costs for dinner must be deducted from your individual vouchers. The per diem amount to be deducted is \$31.00.

b7E

Attendees should make reservations at the [REDACTED]. The [REDACTED] telephone number for reservations is [REDACTED].

If you are choosing to stay at another area hotel, you are reminded, due to high occupancy rates, U.S. Government per

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 10/27/2008

b7E

diem rate rooms may be unavailable. It is requested that attendees make reservations as soon as possible.

VOUCHERS

Vouchers for travel relative to this training will be charged to a travel authorization number to be provided at a later date. Rental vehicles will not be authorized for this TR number. The cost of rental vehicles must be carried by the individual attendee or the attendee's field office. Third Party Draft officials shall not authorize any vehicle rentals under the provided TR number.

The maximum allowance for lodging in the Arlington, VA area while on U.S. Government official business is \$209.00 per night. The allowance for miscellaneous and incidental expenses (M&IE) is \$64.00 per day.

TRAVEL AND TRANSPORTATION

If traveling by air, attendees are encouraged to utilize Ronald Reagan Washington National Airport. The Washington, D.C., metro system blue line will take attendees from the airport to the Metro Center stop.

ATTENDANCE

As is customary at in-service training, attendance is mandatory for all seminar sessions. If an absence is unavoidable, contact the [REDACTED] at [REDACTED]. This requirement is to ensure that the attendee is in an on-duty status and will provide the attendee the appropriate protection in the event of an emergency.

b6
b7C
b7E

IN-SERVICE TRAINING AND REGISTRATION

Virtual Academy and FBI e-mail will be the mechanism to register for this seminar.

The course is listed as the CI Executive Management Seminar in the Virtual Academy.

CITC requests that all attendees complete the following as soon as possible:

- (1) Register through the Virtual Academy.

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 10/27/2008

b6
b7C
b7E

(2) Via internal FBI e-mail to
SSA [REDACTED] CITC, CD, using
the subject "*CI Executive Management Seminar*",
provide the following information:

- (a) Official Bureau Name and Title
- (b) SSAN
- (c) Field Office Assignment and telephone
number(s) for further contact
- (d) Name and contact information for USIC
personnel if you are nominating one for
attendance to this course

MISCELLANEOUS

Professional business attire is appropriate for this
seminar.

Any employee selected to attend this in-service who may
be in need of a special accommodation (i.e., sign language
interpreter; audio loop; personal assistant; large print
materials; etc.) should contact [REDACTED]
[REDACTED] as soon as possible.

b6
b7C

Any questions concerning this seminar should be
directed to the following CITC personnel;

[REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 10/27/2008

b7E

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

(U) 1. Division Training Coordinators need to input the attendees' information into the Virtual Academy under the *CI Executive Management Seminar*.

(U) 2. Attendees need to provide via the internal FBI email the following information to SSA [REDACTED] CITC, CD, using the title "*CI Executive Management Seminar*" no later than November 21, 2008:

b6
b7C

- (a) Official Bureau Name and Title
- (b) SSAN
- (c) Field Office Assignment and telephone number(s) for further contact
- (d) Name and contact information for USIC personnel if you are nominating one for attendance to this course

♦♦

UNCLASSIFIED

~~SECRET~~



DATE: 01-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-09-2037

Counterintelligence Executive Management Seminar

December 1 - 4, 2008

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Monday, December 1st

8:30am - 8:45am

Welcome to FBI Counterintelligence Training

(confirmed)

[redacted]
[redacted] Supervisory Special Agent
[redacted] Supervisory Special Agent (confirmed)
Counterintelligence Training Center

b6
b7C

8:45am - 9:45am

Counterintelligence Division

Stephanie Douglas, Deputy Assistant Director (confirmed)
Richard DesLauriers, Deputy Assistant Director (confirmed)
Counterintelligence Division

10:00am - 10:30am

FBI Trends and Initiatives

Robert S. Mueller III, Director (confirmed)

10:30am - 11:00am

FBI Trends and Initiatives

John S. Pistole, Deputy Director (confirmed)

11:00am - 11:45am

National Security Branch

Arthur M Cummings II, Executive Assistant Director (confirmed)

11:45am - 12:30pm

Cyber Division

Shawn Henry, Assistant Director (confirmed)

b6
b7C

12:30pm - 1:30pm

Lunch

1:30pm - 2:15pm

Understanding the Threat

[redacted] Assistant Section Chief, Analytical Section
(confirmed)

2:30pm - 4:30pm

What to do about the Threat: CD Section Unified Battle Plan

Jill Marie Eulitz, Section Chief, Eurasia Section (confirmed)
Randall C. Thysse, Section Chief, Global Section (confirmed)
Keith D. Salette, Acting Section Chief, East Asia Section

(confirmed)

4:30pm

Wrap-up

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

December 1 - 4, 2008

Tuesday, December 2nd

8:00am - 12:00pm

Value of Sophisticated Operations

[Redacted]

Eurasia Section (confirmed)

[Redacted]

Special Agent, Washington Field Office

(confirmed)

Guest Speaker (confirmed)

b6
b7C

12:00pm - 1:00pm

Lunch

1:00pm - 2:00 pm

[Redacted]

[Redacted]

(S)

b1
b6
b7C
b7E

2:00pm - 2:30pm

[Redacted]

2:30pm - 3:30pm

Self-Guided Cold War Exhibit Tour and Store

3:45pm - 4:45pm

Round Table Discussion, Best Practices

Seminar Attendees (confirmed)

4:45pm - 5:15pm

Counterintelligence Center, Counterespionage Group

[Redacted]

(S)

5:15pm - 6:30pm

Reception

6:30pm - 7:30pm

[Redacted]

(S)

b1
b7E

7:30pm - 8:00pm

Return travel to FBIHQ via bus

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

December 1-4, 2008

Wednesday, December 3rd

8:30am - 9:30am *Counterespionage Issues*
Robert Anderson, Jr., Section Chief, Counterespionage Section

9:30am - 11:30am *Legal Authorities*
[Redacted]
National Security Law Branch

11:45am - 12:30pm *Managing Change in the FBI*
[Redacted] McKinsey & Associates

12:30pm - 1:30pm *Lunch*

1:30pm - 2:30pm *Confidential Human Source Validation: Vital & Essential*
Dolores Gilbert, Section Chief, [Redacted]
[Redacted]

2:45pm - 3:45pm *Domain Initiatives: Engaging in Strategic Partnerships;
Working with the Academic and Business Alliances*
David Varner, Acting Assistant Section Chief (confirmed)
[Redacted] Section

3:45pm - 4:30pm *Regional Counterintelligence Working Groups: Best Practices*
David Varner, Acting Assistant Section Chief (confirmed)
[Redacted] Section

4:30pm *Wrap up*

b6
b7C

b7E

~~SECRET~~

Counterintelligence

ACLURM042014

FBI040914

~~SECRET~~

Executive Management Seminar

December 1-4, 2008

Thursday, December 4th

8:30am - 9:30am *Office of the Director of National Intelligence*
John J. Hess, Associate Director of National Intelligence
Senior Ranking FBI Detailee to [] (confirmed)

9:30am - 10:30am *Weapons of Mass Destruction Directorate: Counterproliferation*
Roland Mignone, Deputy Assistant Director (confirmed)

10:30am - 11:30am *Counterterrorism Division*
Michael Heimbach, Assistant Director

11:30am - 12:30pm [] *Resources*
[]
Operations Support to the IC, Special Projects
[]

12:30pm - 1:30pm *Lunch*

1:30pm - 2:30pm *Directorate of Intelligence*
Kevin Favreau, Assistant Director (confirmed)

2:30pm - 3:30pm *Closing Remarks*
Daniel Lee Cloyd, Assistant Director (confirmed)
Counterintelligence Division

3:30pm *Wrap up*

b6
b7C
b7E

~~SECRET~~

UNCLASSIFIED//FOR OFFICIAL USE
ONLY

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-06-2012 BY 65179 DMH/STW

~~SECRET~~



UNCLASSIFIED//FOR OFFICIAL USE ONLY

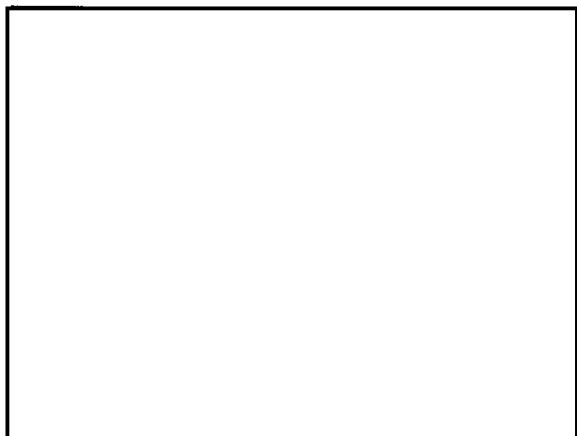
[Redacted]

**Slides are classified as noted.
Discussion in support
of these slides may exceed the
classification level indicated.**

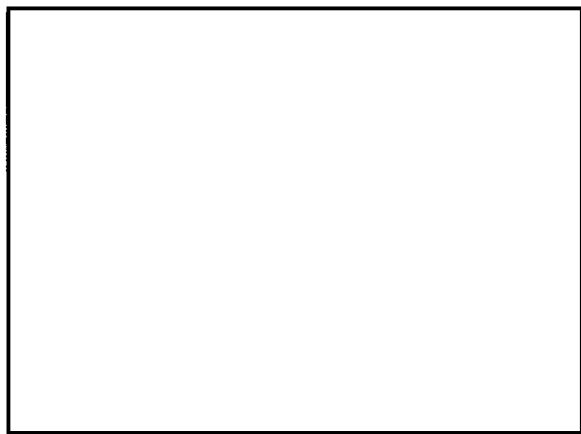
13 July 2011

UNCLASSIFIED//FOR OFFICIAL USE ONLY

b7E



b7E



b7E

UNCLASSIFIED//FOR OFFICIAL USE
ONLY

~~SECRET~~

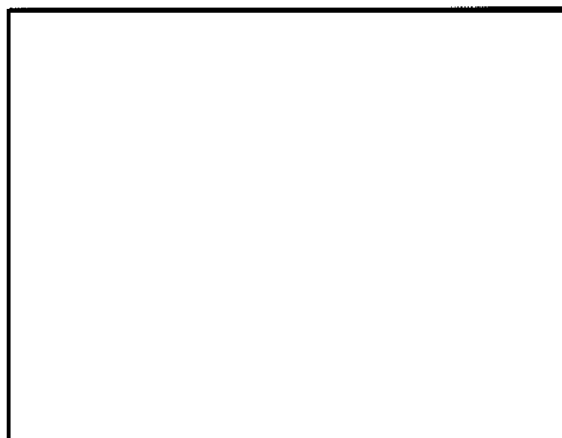
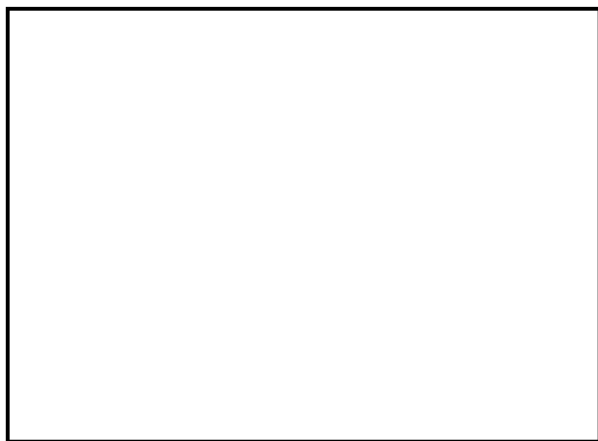
UNCLASSIFIED//FOR OFFICIAL USE
ONLY



b7E



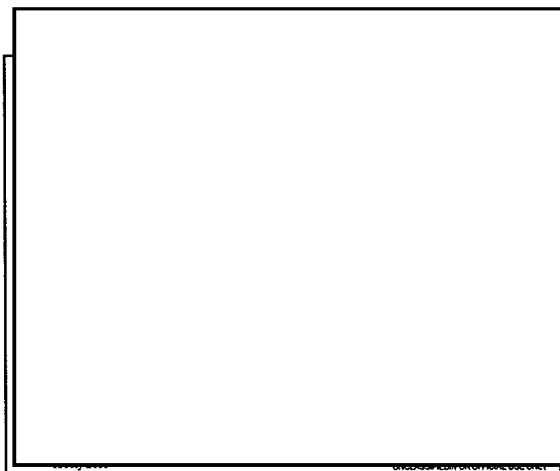
b7E



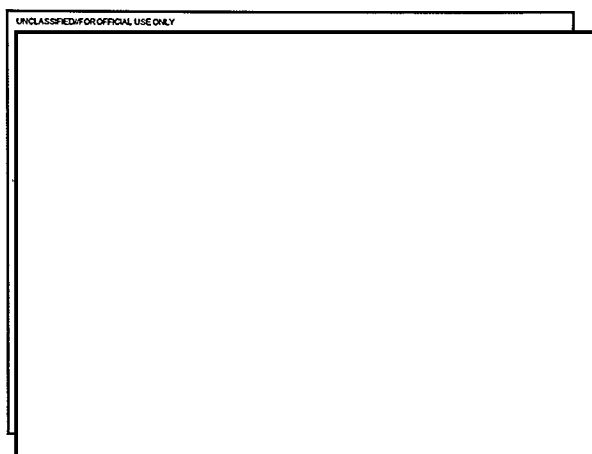
b7E

UNCLASSIFIED//FOR OFFICIAL USE
ONLY

UNCLASSIFIED//FOR OFFICIAL USE
ONLY



b7E



b7E



b7E

UNCLASSIFIED//FOR OFFICIAL USE
ONLY

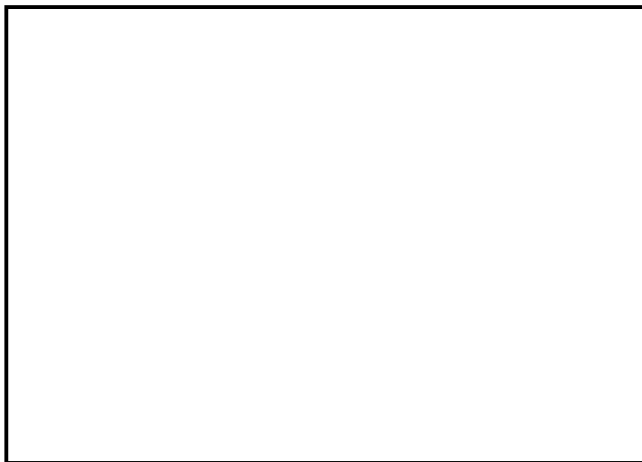
FDPS pg
256

ACLURM042018

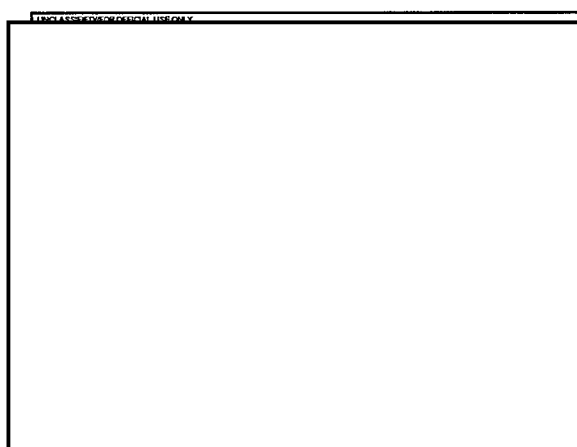
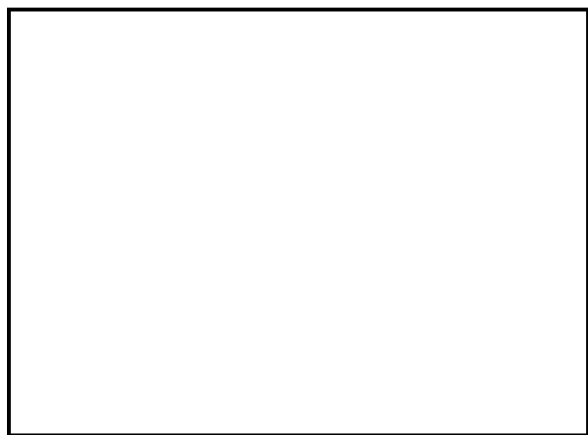
3

FBI040918

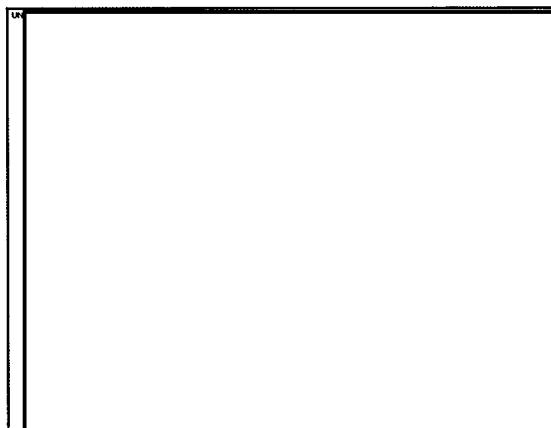
UNCLASSIFIED//FOR OFFICIAL USE
ONLY



b7E



b7E



b6
b7C
b7E

UNCLASSIFIED//FOR OFFICIAL USE
ONLY

FDPS pg
257

ACLURM042019

[illegible]

UNCLASSIFIED//FOR OFFICIAL USE ONLY	
RESPONSIBILITIES	

FBI040920

~~SECRET~~

DATE: 01-10-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DISCOVERY REQUEST MATERIAL

COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR

JUNE 1-4, 2009

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

June 1 - 4, 2009

Attendees

Agency

Telephone Number

(S)

b1
b6
b7C
b7E

[Redacted]		[Redacted]
[Redacted]		
[Redacted]		
[Redacted]		[Redacted]
[Redacted]		
[Redacted]		
[Redacted]		
[Redacted]		
[Redacted]		
[Redacted]		

~~SECRET~~

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-06-2011 BY 65179 DMH/STW

Precedence: DEADLINE 09/15/2009

Date:

To: All Field Offices

Attn: SAC
NSB ASAC
Training Coordinator

From: Counterintelligence

Contact: SSA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

kd

Case ID #: [REDACTED] (Pending)

Title: COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR;
COUNTERINTELLIGENCE DIVISION;
COUNTERINTELLIGENCE TRAINING CENTER;
JUNE 1 - 4, 2009;
FBIHQ, STRATEGIC INFORMATION AND OPERATIONS CENTER

Synopsis: To advise receiving offices of captioned seminar and to provide registration and administrative information.

Details: The Federal Bureau of Investigation (FBI) National Strategy for Counterintelligence (CI) mandates an increased focus on both the professionalization of the FBI CI workforce, and the training required to establish that professionalized cadre. As part of this training, the Counterintelligence Division's (CD) Counterintelligence Training Center (CITC) has developed and mandated a CI Executive Management Seminar for all Special Agents-in-Charge (SACs) and Assistant Special Agents-in-Charge (ASACs) who are overseeing CI operations, have not already attended this seminar, and are not considered CI proficient. The seminar will focus on various topics outlined in the National Strategy for CI.

CI proficiency for Executive Managers is defined as three (3) years in the CI program and two (2) CI courses of any kind, either FBI or United States Intelligence Community (USIC) sponsored.

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] ??

b7E

While the seminar is open to all field executives, preference will go to those executives with CI program oversight responsibilities. The seminar is being held at FBIHQ in the Strategic Information and Operations Center (SIOC). Space is limited to 30 seats.

In an effort to foster continuing collaboration with our USIC partners, CITC has opened this seminar to the USIC. If you are attending this course and would like to nominate an equivalent executive (GS-15/SES) from the USIC, with whom you regular liaise, please forward the name to CITC along with your registration information. CITC will work with the agency's training entity to ensure the appropriate USIC representatives are invited and selected to attend. Your nomination will help CITC to identify those candidates currently working with the FBI in the field; however, final selection will be made by CITC. While the FBI will cover materials and course fees for the USIC attendees, the travel and per diem costs must be incurred by the individual agencies.

COURSE LOCATION AND DURATION

The CI Executive Management Seminar will be held in the [REDACTED] FBIHQ. The seminar will start promptly at 8:30 AM on Monday, June 1, 2009 and will end at approximately 5:00 PM on Thursday, June 4, 2009.

b7E

Sunday, May 31, 2009 is the designated travel day for this seminar. If possible, no travel arrangements should be made with a departure time prior to 6:00 PM, Thursday, June 4, 2009.

On Wednesday, June 3, 2009, there will be an evening event at the [REDACTED]. Transportation to and from this event will be provided. As food will be provided, per diem costs for dinner must be deducted from your individual vouchers. The per diem amount to be deducted is \$31.00.

b7E

Attendees should make reservations at the [REDACTED]
[REDACTED]
The telephone number for reservations is [REDACTED]
Reservations need to be made by May 10, 2009 as the hotel will release all rooms not reserved.

b7E

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] ??

b7E

As the FBI has signed a letter of intent for the hotel, attendees should make every attempt to stay at the [REDACTED]. If you are choosing to stay at another area hotel, you are reminded, due to high occupancy rates, U.S. Government per diem rate rooms may be unavailable. It is requested that attendees make reservations as soon as possible.

VOUCHERS

b7E

Vouchers for travel relative to this training will be charged to travel authorization number (TR) [REDACTED]. Rental vehicles will not be authorized for this TR number. The cost of rental vehicles must be carried by the individual attendee or the attendee's field office. Third Party Draft officials shall not authorize any vehicle rentals under the provided TR number.

The maximum allowance for lodging in the Arlington, VA area while on U.S. Government official business is \$209.00 per night. The allowance for miscellaneous and incidental expenses (M&IE) is \$64.00 per day.

TRAVEL AND TRANSPORTATION

If traveling by air, attendees are encouraged to utilize Ronald Reagan Washington National Airport. The Washington, D.C., metro system's yellow line will take attendees from the airport to the Crystal City stop where an underground walkway will direct attendees to the hotel. The metro system's yellow line will also provide attendees transportation to FBIHQ via the Archive/Navy Memorial stop.

ATTENDANCE

As is customary at in-service training, attendance is mandatory for all seminar sessions. If an absence is unavoidable, contact the [REDACTED] at [REDACTED]. This requirement is to ensure that the attendee is in an on-duty status and will provide the attendee the appropriate protection in the event of an emergency.

b6
b7C

IN-SERVICE TRAINING AND REGISTRATION

Virtual Academy and FBI e-mail will be the mechanisms to register for this seminar.

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] ??

b7E

The course is listed as the CI Executive Management Seminar in the Virtual Academy.

CITC requests that all attendees complete the following as soon as possible:

- (1) Register through the Virtual Academy.
- (2) Via internal FBI e-mail to SSA [REDACTED] CITC, CD, using the subject "CI Executive Management Seminar," provide the following information:
 - (a) Official Bureau Name and Title
 - (b) SSAN
 - (c) Field Office Assignment and telephone number(s) for further contact
 - (d) Name and contact information for USIC personnel if you are nominating one for attendance to this course

b6
b7C

MISCELLANEOUS

Professional business attire is appropriate for this seminar.

Any employee selected to attend this in-service who may be in need of a special accommodation (i.e., sign language interpreter; audio loop; personal assistant; large print materials; etc.) should contact [REDACTED] as soon as possible.

b6
b7C

Any questions concerning this seminar should be directed to the following CITC personnel:

[REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] ??

b7E

LEAD(s) :

Set Lead 1: (Action)

ALL RECEIVING OFFICES

(U) 1. Division Training Coordinators need to input the attendees' information into the Virtual Academy under the *CI Executive Management Seminar*.

(U) 2. Attendees need to provide via the internal FBI email the following information to *SSA* [REDACTED] CITC, CD, using the title "*CI Executive Management Seminar*," no later than May 20, 2009:

b6
b7C

- (a) Official Bureau Name and Title
- (b) SSAN
- (c) Field Office Assignment and telephone number(s) for further contact
- (d) Name and contact information for USIC personnel if you are nominating one for attendance to this course

♦♦

UNCLASSIFIED

~~SECRET~~

DATE: 01-10-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DISCOVERY REQUEST MATERIAL

COUNTERINTELLIGENCE EXECUTIVE MANAGEMENT SEMINAR

SEPTEMBER 28 - OCTOBER 1, 2009

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

September 28 - October 1, 2009

Attendees

Agency

Telephone Number

--	--	--

b6
b7C
b7E

~~SECRET~~

~~SECRET~~

Counterintelligence Training Center

Please complete this form to to insure training credit is recorded.

Class Name: CI Executive Management Seminar 09-03

TR #

Travel Dates: 9/27/2009

Class Dates: 09/28 - 10/01/09

Class Location: SIOC

Class Coordinator:

Section/Unit Sponsor:

Notes:

*	*	*	*	*	*
Last Name	First Name	MI	Title	FO	

--	--	--	--	--	--

b6
b7C
b7E

--	--	--	--	--	--

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

*FBIHQ, Strategic Information and Operations Center
September 28 - October 1, 2009*

Monday, September 28

8:30am - 8:45am

Welcome to FBI Counterintelligence Training

[Redacted]

[Redacted]

[Redacted]

Supervisory Special Agent

Supervisory Special Agent

Counterintelligence Training Center

b6
b7C

8:45am - 9:45am

Counterintelligence Division

Richard DesLauriers, Deputy Assistant Director

Jill Marie Eulitz, Deputy Assistant Director

Counterintelligence Division

10:00am - 10:30am

FBI Trends and Initiatives

Robert S. Mueller III, Director

10:30am - 11:00am

FBI Trends and Initiatives

John S. Pistole, Deputy Director

11:15am - 11:45am

Administrative and Introductions

[Redacted]

Supervisory Special Agent

Seminar Attendees

b6
b7C

11:45am - 1:00pm

Lunch

1:00pm - 1:30pm

Understanding the Threat

Kenneth B. Pack, Acting Section Chief,

Counterintelligence Analysis Section

1:30pm - 3:30pm

What to do about the Threat: CD Section Unified Battle Plan

William R. Evanina, Acting Section Chief, Eurasian Section

Randall C. Thysse, Section Chief, Global Section

Frank Montoya, Jr., Section Chief, East Asia Section

3:30pm - 4:30 pm

Counterespionage Issues

Robert Anderson, Jr., Section Chief, Counterespionage Section

4:30pm

Wrap-up

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

***FBIHQ, Strategic Information and Operations Center
September 28 - October 1, 2009***

Tuesday, September 29th

8:30am - 9:30am	<i>Domain Initiatives: Engaging in Strategic Partnerships; Working with the Academic and Business Alliances</i> J. Chris Woiwode, Section Chief Counterintelligence Program Coordination Section
9:30am - 10:15am	<i>Regional Counterintelligence Working Groups: Best Practices</i> J. Chris Woiwode, Section Chief Counterintelligence Program Coordination Section
10:15am - 11:00am	<i>Counterintelligence Training Initiatives</i> Counterintelligence Training Center
11:00am - 11:45am	<i>Clandestine Services Initiatives</i> Peter Georgacopoulos, Section Chief, Clandestine Services Section
11:45am - 1:00pm	<i>Lunch</i>
1:00pm - 2:00pm	<i>Legal Authorities</i> National Security Law Branch
2:00pm - 3:15pm	<i>Legal Initiatives for Counterintelligence Investigations</i> Steven W, Pelak, Principal Deputy Chief, Counterespionage Section Department of Justice
3:30pm - 4:30pm	<i>Counterterrorism Division</i> Michael J. Heimbach, Assistant Director
4:30pm	<i>Wrap up</i>

b6
b7C
b7E

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

*FBIHQ, Strategic Information and Operations Center
September 28 - October 1, 2009*

Wednesday, September 30th

8:30am - 11:45am *Value of Sophisticated Operations*
William R. Evanina, Acting Section Chief, Eurasian Section
Guest Speaker

11:45am - 1:00pm *Lunch*

1:00pm - 2:00pm *Office of the Director of National Intelligence*
John J. Hess, Associate Director of National Intelligence
Senior Ranking FBI Detailee to [redacted]

b6
b7C
b7E

2:00pm - 2:45pm [redacted]
[redacted] Assistant Director

2:45pm - 3:15pm [redacted]

3:15pm - 3:45 pm [redacted]

4:00pm - 4:30pm [redacted]

(S)

b1
b7E

4:30pm - 6:00pm *Reception*

(S) 6:00pm - 7:00pm [redacted]

7:00pm *Return travel to FBIHQ via bus*

~~SECRET~~

~~SECRET~~



Counterintelligence Executive Management Seminar

*FBIHQ, Strategic Information and Operations Center
September 28 - October 1, 2009*

Thursday, October 1st

(S) 8:30am - 9:30am *National Security Agency*
[Redacted]
[Redacted] Representative to FBI

9:30am - 10:30am *Cyber Division*
Shawn Henry, Assistant Director

10:45am - 11:45am *Weapons of Mass Destruction Directorate*
Vahid Majidi, Assistant Director

11:45am - 1:00pm *Lunch*

1:00pm - 2:00pm *Confidential Human Source Validation: Vital & Essential*
[Redacted]
Intelligence Operations and Oversight
Directorate of Intelligence

2:00pm - 3:00pm *Directorate of Intelligence*
Kevin Favreau, Assistant Director

3:15pm - 4:00pm *Closing Remarks*
Daniel Lee Cloyd, Assistant Director
Richard DesLauriers Deputy Assistant Director,
Jill Marie Eulitz, Deputy Assistant Director
Counterintelligence Division

4:00pm *Wrap up*

b1
b6
b7C
b7E

~~SECRET~~

(S)

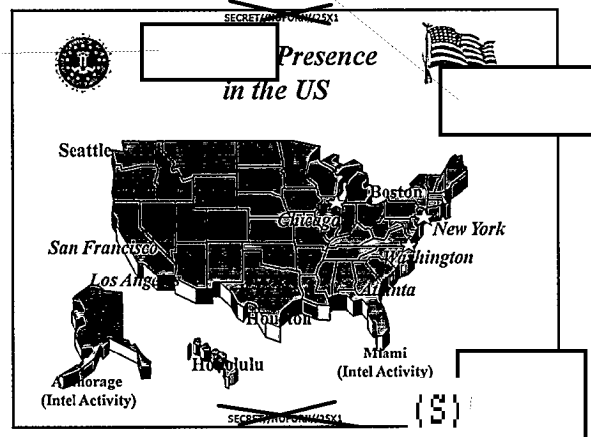
(S)

b1
b7E

(S)

(S)

(S)

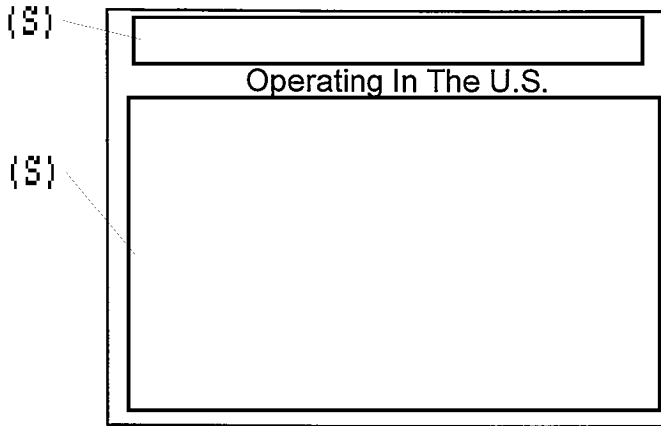


b1
b7E

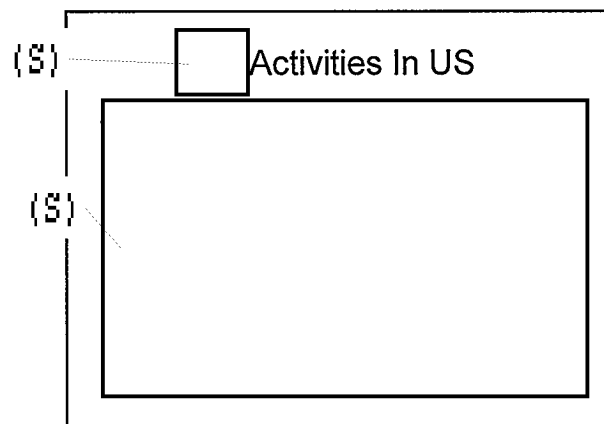
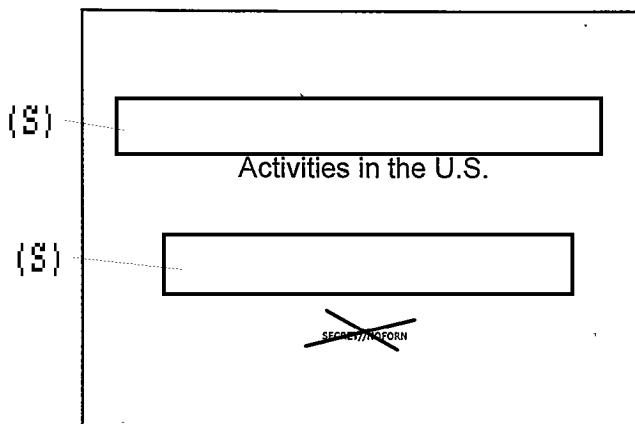
(S)

(S)

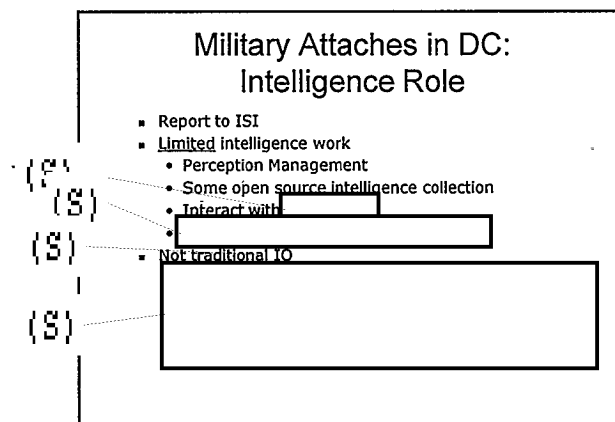
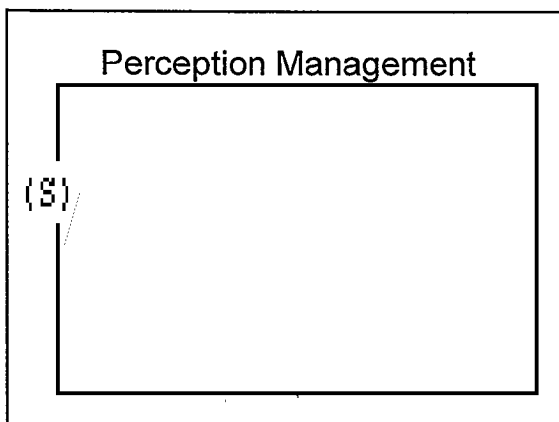
b1
b7E



b1
b7E



b1
b7E



b1
b7E

(S) [Redacted] Intelligence
Activities in the U.S.

(S) [Redacted]

~~SECRET//NOFORN~~

(S) [Redacted]

~~SECRET//NOFORN~~

b1
b7E

(S) [Redacted]

(S) [Redacted]

~~SECRET//NOFORN~~

b1
b7E

(S) [Redacted]

~~SECRET//NOFORN~~

(S) [Redacted]

~~SECRET//NOFORN~~

b1
b7E

DATE: 01-10-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-10-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET//NOFORN~~

Understanding the Foreign Intelligence Threat

Presented by
A/Sc [redacted]
September 28, 2009
[redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI Counterintelligence Strategy

[redacted] 

National Counterintelligence Strategy
2007 - 2010

2

~~SECRET//NOFORN~~

b6
b7C
b7E



~~SECRET//NOFORN~~

The Focus

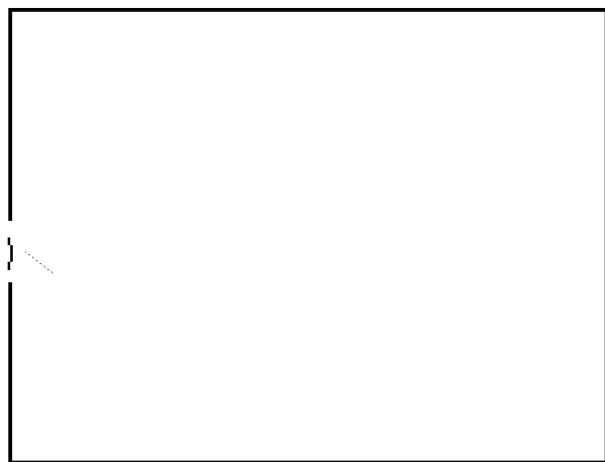
[redacted] 

Counterintelligence Program Operations
Plan for 2008 - 2009

4

~~SECRET//NOFORN~~

b7E



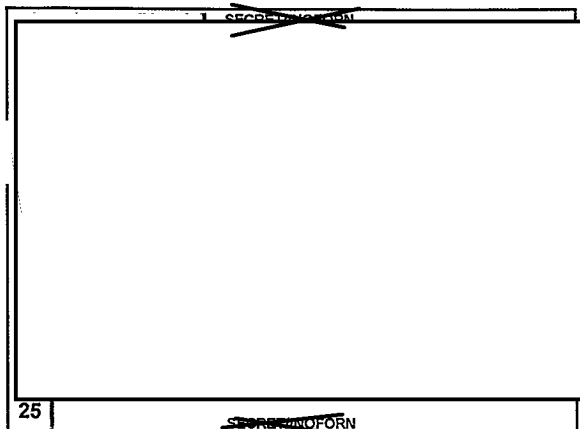
b1
b7E

(S)

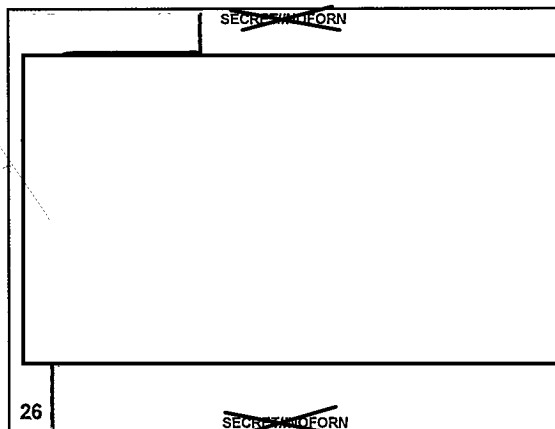
~~SECRET~~

~~SECRET~~

(S)

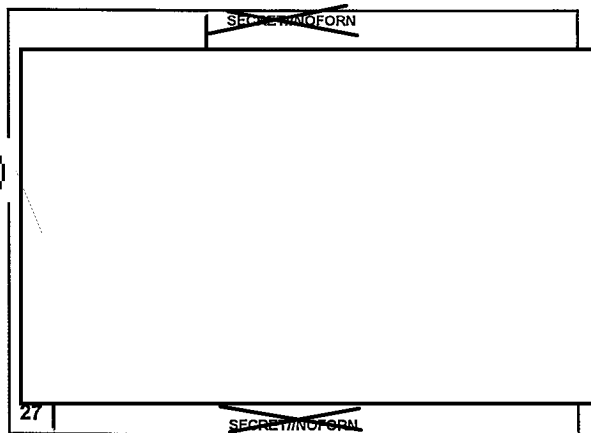


(S)



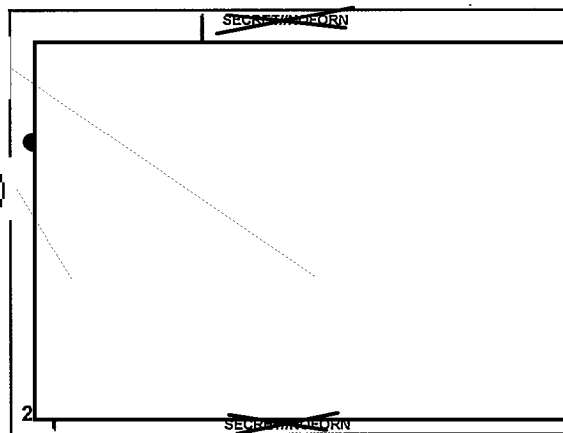
b1
b7E

(S)

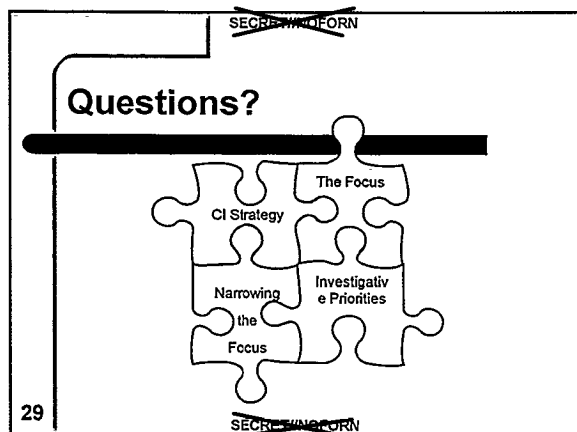


(S)

(S)



b1
b7E



~~SECRET~~

7/13/2011

~~SECRET~~

DATE: 01-10-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

What does CI mean?

"...information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities" (see E.O. 12333 § 3.4(a))

For Official Use Only

ISSUE THREATS

- Espionage (National Defense Information)
- Proliferation (Weapons of Mass Destruction)
- Economic Espionage
- National Information Infrastructure Targeting
- Infiltrating the U.S. Government
- Perception Management
- Foreign Intelligence Activities

b6
b7C

The Evolving Intelligence Threat

(S)

(S)

(S)

(S)

Threat = Presence + Cyber

For Official Use Only

~~SECRET//NOFORN~~

Who's Who...

(U) Criteria - Intent + Capability + Opportunity = Threat

(S)

Quote: "Some 108 countries - a mix of rich and poor, high- and low-tech, friend and foe - targeted U.S. technologies in 2007 totaling \$1.4 billion in losses to the Nation's economic and security sectors..."

2007 Annual Report to Congress
Prepared by the National
Counterintelligence
Executive (NCE)

~~SECRET//NOFORN~~

For Official Use Only

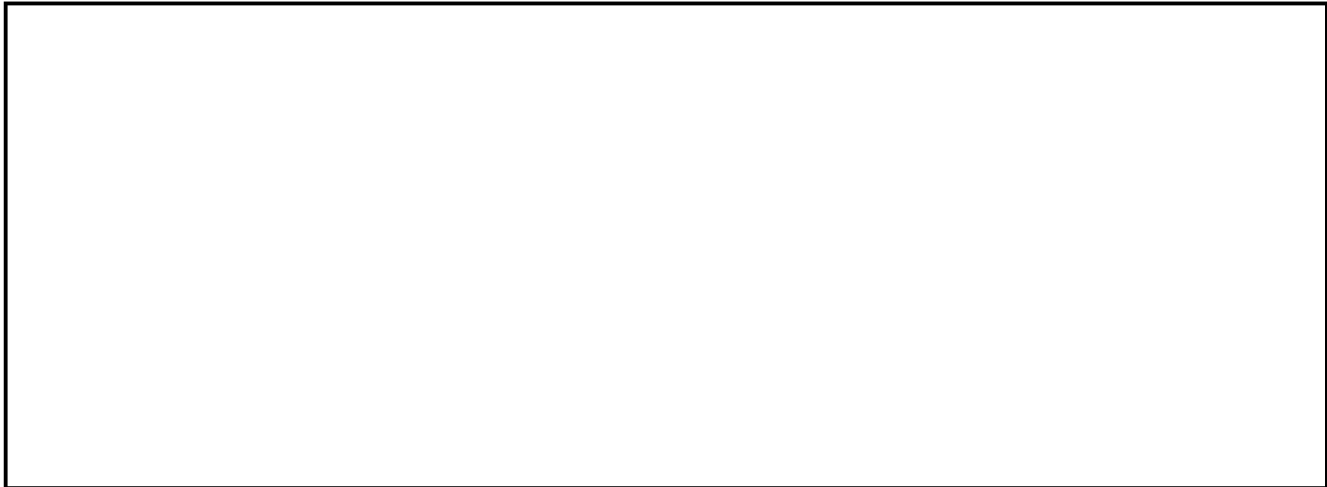
b1
b7E

b7E

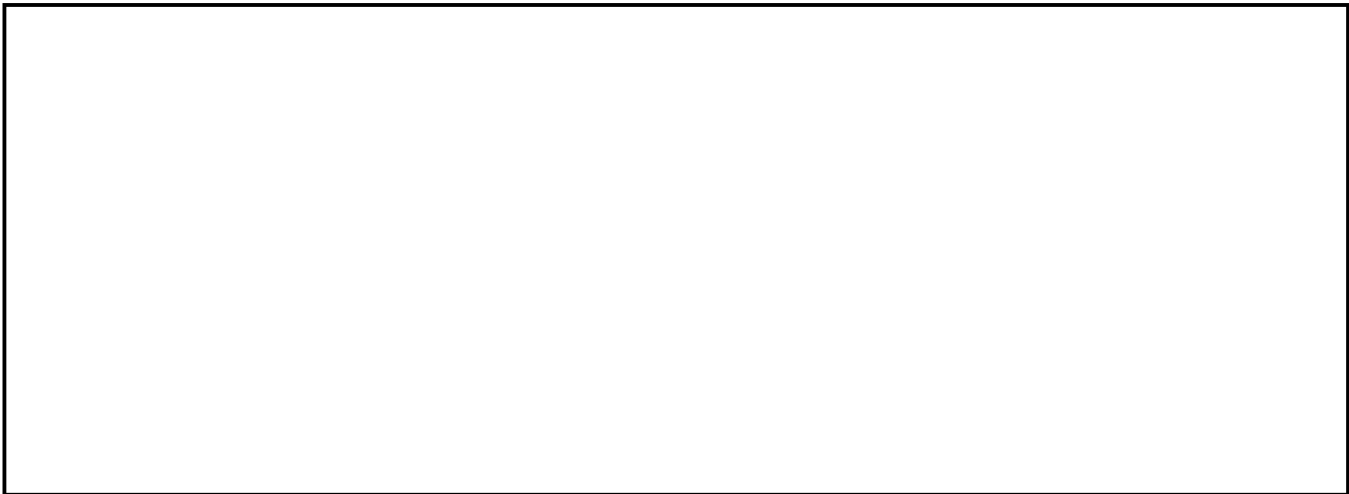
~~SECRET~~

~~SECRET~~

7/13/2011



b7E



~~SECRET~~

Academic Alliances

- Alliances w/ Higher Education/Academia
conducting critical GOV & sensitive research
- Mutual focus:
 - Threat perspectives; cultural awareness &
RISK Management partnerships.
- College and University Security Effort (CAUSE)
- Nat'l Security Higher Education Advisory Board
(NSHEAB)

 Dr. Graham Spanler, President, Penn State University
- Chairman, NSHEAB
- Higher Education Representative, National CI WG

For Official Use Only

Counterterrorism Concerns

- ☐ Foreign students
- ☐ Foreign visitors
- ☐ Large population within limited geography
- ☐ High-profile national and international visitors
- ☐ Eco Terrorism
- ☐ Animal rights terrorism
- ☐ Other causes

For Official Use Only

Counterintelligence Concerns

- ☐ University-produced intellectual property
- ☐ Classified research
- ☐ Unclassified but sensitive research
- ☐ Foreign students
- ☐ Foreign visitors
- ☐ U.S. citizens and permanent residents
- ☐ Deemed exports

For Official Use Only

Cyber Security Threats

- ☐ Viruses, worms, trojans
- ☐ Hacking/Cracking
- ☐ Brute force attacks
- ☐ Identity theft
- ☐ Denial of service attacks
- ☐ Cons/Fraud
- ☐ Disgruntled employees
- ☐ Disruption of infrastructure
- ☐ Openness of university systems
- ☐ University networks as conduits



For Official Use Only

Other Security Matters

- ☐ Campus safety
- ☐ Criminal
- ☐ Sports gambling, organized crime
- ☐ Student safety abroad
- ☐ Intersection of policy and political
 - ☐ Visas
 - ☐ Visiting scholars

For Official Use Only

Academic Alliance Program

- ☐ Foster spirit of cooperation
- ☐ Establish a dialogue
- ☐ Share information
- ☐ Increase awareness



For Official Use Only

Academic Alliance Program Initiatives

- National Security Higher Education Advisory Board (NSHEAB)
Hosted by FBI Headquarters
- College and University Security Effort (CAUSE)

Outreach conducted through the 56 FBI field offices

For Official Use Only

National Security Higher Education Advisory Board

- Members include 20 university presidents and chancellors
- Chaired by President Graham Spanier, The Pennsylvania State University
- Three meetings a year
- Other participants include:
 - National Science Foundation
 - Department of Commerce
 - Central Intelligence Agency
 - Department of Defense

For Official Use Only

Mission of the NSHEAB

- ☐ Create a forum for mutual issues
- ☐ Promote understanding
- ☐ Provide advice on the culture of higher education
- ☐ Build on traditions of openness, academic freedom and international collaboration
- ☐ Discuss matters pertaining to national security

For Official Use Only

NSHEAB Members

President Robert Berdahl
Association of American Universities

Chancellor Criss Blach
University of California, Los Angeles

President Margaret C. Bond
American Council on Education

President Richard H. Brodhead
Duke University

President Jared L. Cohen
Carnegie Mellon University

President Michael Crow
Arizona State University

President Mark Allen Emmert
University of Washington

President Gregory L. Gault
Iowa State University

Chancellor Richard H. Hovland
University of Illinois at Urbana-Champaign

President David L. Kirsh
Rice University

President L. Bernard Natchez
University of Florida

President C.D. Voss, Jr.
University of Maryland-College Park

President G.P. Peterson
Georgia Institute of Technology

President William C. Powers
University of Texas at Austin

President John Sexton
New York University

President Lee Anna K. Shaw
Michigan State University

President David Shulman
Cornell University

President Graham B. Spanier
The Pennsylvania State University

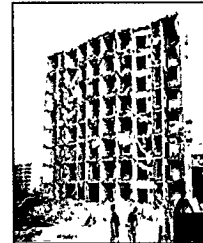
Chancellor Mark Stephen Wiegman
Vanderbilt University

Chancellor Nancy L. Zingales
The State University of New York

For Official Use Only

NSHEAB Agenda Topics

- ☐ Counterterrorism
- ☐ Counterintelligence
- ☐ Cyber crimes
- ☐ Animal Liberation
Front/Earth Liberation
Front
- ☐ Deemed Exports
- ☐ Buckley Amendment
- ☐ Patriot Act



For Official Use Only

College and University Security Effort

- ☐ Foster spirit of cooperation
- ☐ Establish a dialogue
- ☐ Share information
- ☐ Increase awareness
- ☐ Conduct outreach
... at the local level



For Official Use Only

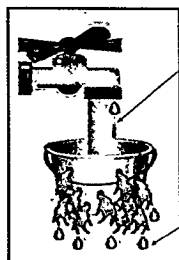
Lessons Learned from Academe

- We recognize that:
- ☐ Knowledge knows no boundaries.
 - ☐ Global competition is good.
 - ☐ Flow of information is vital.



For Official Use Only

Lessons Learned



New Technology/R&D

Old Technology/R&D

For Official Use Only

National Security Concerns Within Academe

- University produced intellectual
- Classified research
- Unclassified but sensitive research
- Cyber intrusions
- R&D related to Weapons of Mass Destruction
- Dual use technology
- Deemed exports



For Official Use Only

“Need to Know” Principle

- What is the impact on U.S. technologies or trade secrets?
- Who needs to know?
- Why am I receiving this request?
- Why is someone demonstrating a great interest?
- How much information is needed to answer the request?
- How much access do people really need on this project?
- What can I do to protect the university's interests?

Remember, researchers could be approached anywhere for information.

For Official Use Only

Collection Techniques

- Email, fax, telephone
- Unsolicited requests and visits
- International conventions, symposiums and meetings
- Exploiting information available on the internet
- Exploiting foreign visitors
- Exploiting family, work relationships
- Exploiting ideology



For Official Use Only

Proactive Measures

- ✓ Report suspicious activities
- ✓ Know countries may target your technology and research
- ✓ Understand military or dual uses
- ✓ Prevent unnecessary access
- ✓ Be cautious in responding to requests for information

For Official Use Only

Challenges

- Different cultures
- Cognizant of history, suspicions
- Academics question everything
- Atmosphere of openness and sharing of ideas

For Official Use Only

Bringing it Home



For Official Use Only

CNAs / Mandate

Presidential Decision Directive (PDD) 75

- Identifies CI support to the protection of R&D and technology as specific mission area

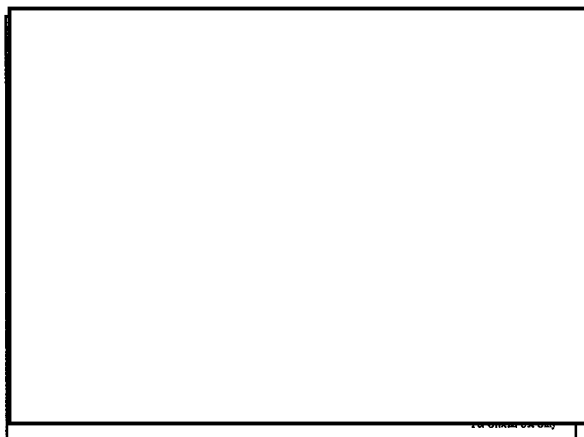
National Counterintelligence Executive (NCIX)

- Requests FBI provide national coordination of proactive counterintelligence support of CNAs in five sectors.

FBI National Strategy

- FBI will partner withUSIC, non-USIC USG Agencies and private sector to prevent the compromise of CNAs.
- Critical National Assets Integrated Counterintelligence Coordination (CNAICC) Unit: Partners with government and private sector stakeholders to facilitate the identification of their CNA's; and then coordinates and enables integrated proactive counterintelligence support.

For Official Use Only

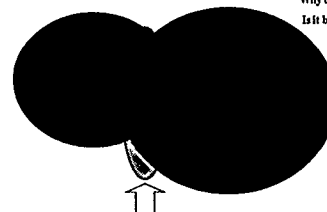
b6
b7C
b7E

For Official Use Only

(Identification & Prioritization)

What is it?
Who owns it?
Where is it?

What do they need?
Why do they need it?
Is it being targeted?



Counterintelligence Zone of
Engagement

For Official Use Only

b7E

Bottom line...

"It's all about relationships"

- Maintain U.S./Allied dual-use and leading-edge military technology superiority...
- Optimize capital investments in U.S. industry...
- Prevent compromise of Critical Research and Technologies...
- Ensure technological advantage to the U.S./Allied warfighter and avoid technology surprise in the battlespace...
- Ensure U.S. economic competitiveness...

For Official Use Only

Final Thoughts

- Business Alliance and NSBAC leaders understand that the FBI is focused on helping protect US companies, employees and shareholders.
- A robust relationship formed prior to the break of an espionage case will be a valuable asset in establishing the trust necessary for successful case conclusion.
- Essential to identify key personnel/stakeholders in the private sector and USG as soon as possible (CI Strategic Partnership Coordinators are valuable assets for this purpose).

For Official Use Only



CI Domain Program Strategic Planning

- Counterintelligence Program Reviews

(S)

For Official Use Only



Field Offices Reviewed FY 2009

• Cincinnati	*Atlanta
• Albany	*Phoenix
• Denver	*Columbia
• Newark	*Portland
• Salt Lake City	*San Diego
• Charlotte	*Honolulu
*Pending Review	

For Official Use Only

b1
b7E

Program Review Process

- Conducted by highly experienced CI SMEs
- Interview based
- Low profile/impact on field office
- Results briefed to FBI executives
- Remediation

For Official Use Only



QUESTIONS?

J. Chris Woiwode
Section Chief, Room 5173

For Official Use Only

b6
b7C

RCIWG

For Official Use Only



Section Chief J. Chris Woiwode

CI Program Coordination Section
Regional CI Working Groups

For Official Use Only

Where do cases come from?

- From relationships with mutual stakeholders who have SME and vested interest in a significant part of the predicated activity

For Official Use Only

Participants

For Official Use Only

b7E

Frequency

What is too often and too seldom?

Quarterly or Monthly?

You decide, what is going to make you understand your domain. Then pulse the domain on a regular basis

For Official Use Only

Some ideas to get started

- Federal Partner (NOT OGAs) Briefing
 - We are _____
 - We are experts at _____
 - _____ keeps us up at night
 - _____ is helpful
 - _____ is not helpful
 - We care about _____
 - We can help the community by _____

For Official Use Only

Possible Initiatives

(S)

For Official Use Only

Some more things to consider

(S)

- Come up with way points and then move on
- IDing no threat is okay

For Official Use Only

b1
b7E

No freeloading

- Share case info when possible with those that have any mutual interest (TT and P and sources excluded)
- Many partners feel their work is not as dynamic as the FBI and are reluctant to share.
- If your squads are not participating, how does that reflect on the importance to our partners

For Official Use Only

b7E

History Continued

- Proposed Agenda

- FBI presentation of:

- Use of visitors, students, émigré etc
 - [redacted] of the domain
 - [redacted] from last 30 days

- Partner agency's presentation of:

- mission, [redacted] staffing level

For Official Use Only

b1
b7E

Current

- Three meetings per year
- Broader participation
- Closely monitored by CD on SAC Participation for PAR
- SAC/SSA facilitator/SA co-facilitator (new)
- Move the meetings around region to accommodate other constituencies such as BA and AA

For Official Use Only

b7E

~~SECRET~~

7/13/2011



b7E

FY 2009

For Official Use Only

FY 2010

For Official Use Only

b7E

FY2010 Fiscal Allocation

- Region 1 ≈
- Region 2 ≈
- Region 3 ≈
- Region 4 ≈
- Region 5 ≈
- Region 6 ≈
- Region 7 ≈
- Region 8 ≈
- Region 9 ≈

Total ≈

For Official Use Only

Region 2 Attendance

Only

b7E

~~SECRET~~

Region 2 Leadership Involvement

Region 2

Leadership Involvement

	1/1-4/2008	4/5-7/2008	7/8-10/2008	10/11-1/2009	1/2-4/2009
SAC	100%	100%	100%	100%	100%
NSB ASAC	100%	100%	100%	100%	100%
OS SA	100%	100%	100%	100%	100%
Other SA	100%	100%	100%	100%	100%
HSA	100%	100%	100%	100%	100%
EPA	100%	100%	100%	100%	100%
Other	100%	100%	100%	100%	100%

Use Only

Region 3 Attendance



Region 3 Attendance

Region 3
11/28/2008 7/14/15/2009

For Official Use Only

b7E

Region 3 Leadership Involvement



Region 3

Leadership Involvement

		Region 3			
		1/28-2/5/2009	2/14-2/20/2009	1/28-2/5/2009	2/14-2/20/2009
SAC				SAC	
NSIR ASAC				NSIR ASAC	
Q SSA				Q SSA	
Ctym SSA				Ctym SSA	
Hem SSA				Hem SSA	
SPC				SPC	
Other				Other	
SAC				SAC	
NSIR ASAC				NSIR ASAC	
Q SSA				Q SSA	
Ctym SSA				Ctym SSA	
Hem SSA				Hem SSA	
SPC				SPC	
Other				Other	
SAC				SAC	
NSIR ASAC				NSIR ASAC	
Q SSA				Q SSA	
Ctym SSA				Ctym SSA	
Hem SSA				Hem SSA	
SPC				SPC	
Other				Other	
SAC				SAC	
NSIR ASAC				NSIR ASAC	
Q SSA				Q SSA	
Ctym SSA				Ctym SSA	
Hem SSA				Hem SSA	
SPC				SPC	
Other				Other	
SAC				SAC	
NSIR ASAC				NSIR ASAC	
Q SSA				Q SSA	
Ctym SSA				Ctym SSA	
Hem SSA				Hem SSA	
SPC				SPC	
Other				Other	



Use Only

Region CIWG membership

Each Division

- SAC
- NSB ASAC
- CI SSA
- Cyber SSA
- Intel SSA
- Strategic Partnership Coordinator

For Official Use Only

Possible Meeting Scenario

- Begin 1 p.m.-

[illegible]

- Each group has chairperson, goals and objectives briefed at executive council at the end of the day or beginning of day 2.

For Official Use Only

Possible Meeting Scenario

- Day 2- 8:30-12:30
- Education presentations, i.e. case presentations, HQ briefings, panel discussions.

For Official Use Only

~~SECRET~~

b6
b7C
b7E

CI Exec Mgmt Seminar Report Card

-

For Official Use Only

For Official Use Only

Bottom Line

- Program Goals and Objectives
- SAPRs
- PARs
- Source QSSRs
 - Can we make cases, enhance existing cases and enhance intelligence collections and HUMINT.
 - No silver bullet
 - In CI we have to turn over a lot of rocks to get something worthwhile; these working groups simply bring more rocks for us to turnover

Education/Briefings and Working Groups

For Official Use Only

For Official Use Only

~~SECRET~~

7/13/2011

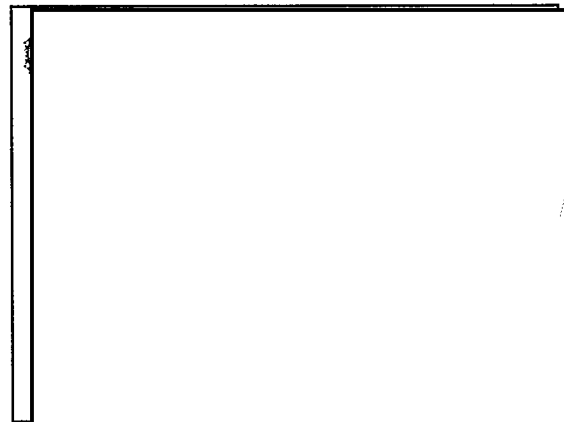
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



A View On the State of the Program

Where we are. And where we need to go.

Frank Montoya, Jr
Section Chief, CD-3
28 September 2009



(S)

b1
b7E



(S)



...And What Have We Been Doing About It?



- Asset Validation
 - Okay, we tried

~~SECRET~~

b1
b7E



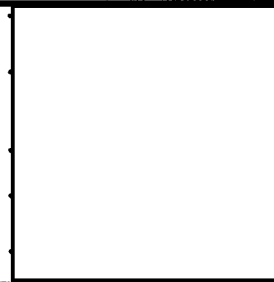
Changing the Paradigm

- Breaking with the Past
 - What is the best way to culminate a case?
 - We are CII (Defense Wins Games)
 - But the Best Defense is a Good Offense
 - Changing the Rules
 - More Tools

~~SECRET~~



Maintaining the "MO"



~~SECRET~~

b7E

~~SECRET~~



A Word on Joint Ops

- Soup of the Day?
- Requires Some Rethinking of Our Role as Type "A's"
- Real Benefits...and not just to our partners.
- Joint Cells

~~SECRET~~



创新

I. Challenges

- Outside
 - AG Exemptions
 - Working with our Partners
- Inside
 - Changing the mindset and overcoming obstacles. Never give up!
 - Understanding the global nature of the effort
 - Working with our Partners
 - Bad Ops v. Good Ops

~~SECRET~~

b7E



We're Here to Help...

I. Specific Guidance:

- a. Asset Travel Overseas
 1. Operational Travel v. Non-Operational Travel
 2. Communications
 3. AD Authority/ICD Approval
 4. Why?
- b. IO identification
- c. Training

~~SECRET~~

(S)

b1
b7E

(S)

~~SECRET/NOFORN~~

Outside Embassy Activity

± Government cover/short term official visitors

(S)

~~SECRET/NOFORN~~

b1
b7E

(S)

Visitors

~~SECRET/NOFORN~~

(S)

Visitors

~~SECRET/NOFORN~~

b1
b7E

(S)

Students/Researchers

~~SECRET/NOFORN~~

(S)

Students/Researchers

~~SECRET/NOFORN~~

b1
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-06-2011 BY 65179 DMH/STW

DOD conference
2003

DATE: 01-10-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 01-10-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FBI Counterintelligence Program

Gulfport Regional Conference
October 27-31, 2003
Gulfport, MS

Change in Emphasis

1. Full understanding of the threat posed by non-
official personnel in the field
2. Focusing operations on priority country and
issues threats.
3. Asserting FBI leadership in the CI Community
4. Eliminating political threats and rebuilding the
capabilities and resource base of the program.
5. Setting and monitoring clear performance
expectations at FBIHQ and in the field.

August 21-22, 2003

CI Eastern Regional Conference

3

b7E

CI Leadership Issues

- What do we mean by leadership of the CI
community?
- Are we generally seen by others in a leadership role?
- What should we be doing to exert leadership that is
not now taking place?
- What limits/constrains our leadership capabilities?
- Where is the equivalent authority of the DCI for
counterintelligence?

August 21-22, 2003

CI Eastern Regional Conference

4

FBI Success

- Identify the objectives, the assets, and the
operations of foreign intelligence services;
- Disrupt their operations
- Change the behavior of targeted institutions
and individuals to minimize opportunities
for exploitation

August 21-22, 2003

CI Eastern Regional Conference

5

b7E

Strategies: What Must Happen

1. Know the Domain
2. Strategic Partnerships
3. Sophisticated CI operations
4. Understand the Threat
5. Engagement of Policy Makers

...at a high level, in every FBI office

August 21-22, 2003

CI Eastern Regional Conference

7

Required Capabilities

- Workforce Expertise
- Sufficient Resources
- Intelligence

...in every FBI office

August 21-22, 2003

CI Eastern Regional Conference

8

Initiative 1: Performance Expectations and Measures

~~SECRET~~

~~SECRET~~

CI Program Strategy
Task: Assess Program-Wide Situation and Set Performance Targets

August 21-22, 2003 CI Eastern Regional Conference 10

Program Assessment

Acceptable ☐ Likely to meet goals

Unacceptable ☐ Making Progress

☐ Significant Problems; Unlikely to meet goals

August 21-22, 2003 CI Eastern Regional Conference 11

Rules

- ☒ Office receives a red rating if any major operational strategy or enabling strategy is red.
- ☐ Office receives a "green" rating if 2 operational strategies and 2 enabling strategies are green and none are red.
- ☐ All other combinations are yellow

Authority: SACs recommend rating; DAD/Section Chiefs concur; AD Approves

August 21-22, 2003 CI Eastern Regional Conference 12

b7E

Hypothetical CI Program Assessment

☒ Unacceptable; Unlikely to meet program goals

August 21-22, 2003 CI Eastern Regional Conference 13

Hypothetical Assessment
Strategy: Know the Domain

August 21-22, 2003 CI Eastern Regional Conference 14

Hypothetical Field Office Plan
Strategy: Know the Domain

August 21-22, 2003 CI Eastern Regional Conference 15

b7E

Example 1: Program Report

Operational Strategies	Perf. Standards	Current Targets
Domain Knowledge	☒	no
Strategic Partnerships	☐	yes
Sophisticated Operations	☒	no
Understand the Threat	☒	yes
Policy Input	☐	yes
Enabling Strategies		
Workforce Expertise	☒	yes
Resource Management	☒	yes
Intelligence	☒	yes

August 21-22, 2003 CI Eastern Regional Conference 16

Example 2: Field Report

	Standards	Targets
Albuquerque	☒	no
Boston	☐	yes
Chicago	☒	no
Kansas City	☒	yes
Houston	☐	yes
Los Angeles	☐	yes
Miami	☒	yes
New York	☒	yes
San Francisco	☒	yes

August 21-22, 2003 CI Eastern Regional Conference 17

Example 3: Office Report

San Francisco FD	Standards	Targets
Domain Knowledge	☒	no
Strategic Partnerships	☐	yes
Sophisticated Operations	☐	yes
Understand the Threat	☒	yes
Policy Input	☐	yes
Enabling Strategies		
Workforce Expertise	☐	yes
Resource Management	☒	yes
Intelligence	☒	yes

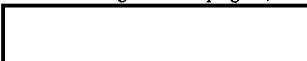
August 21-22, 2003 CI Eastern Regional Conference 18

~~SECRET~~

~~SECRET~~

Conclusion

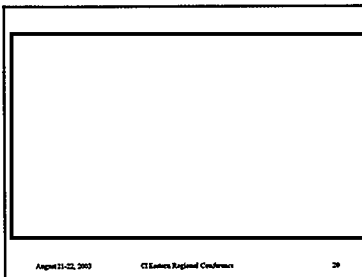
While our performance and capabilities continue to be below the standards we have set for the CI program, the FBI is making substantial progress,



August 11-22, 2003

CI Eastern Regional Conference

19



August 11-22, 2003

CI Eastern Regional Conference

20

Approach

Objective: Substantial progress in each strategy area.

Requirement:

1. Limited movement of specialized expertise in demonstration areas
2. Close oversight
3. Mentoring and training as needed

Candidate Offices:

1. San Francisco
2. Seattle
3. Las Vegas
4. Kansas City
5. Baltimore
6. Norfolk

August 11-22, 2003

CI Eastern Regional Conference

21

b7E

CI Program Strategy



August 11-22, 2003

CI Eastern Regional Conference

22

Strategy Applied:
Baltimore Field Division

Assessment Worksheet: DOMAIN

BALTIMORE FIELD DIVISION ○

Criteria		Current	FY04 Target
WMD	○	38 sites (85%)	45 sites (100%)
Top Secret Cleared	●	38 sites (5%)	700+ sites (75%)
Outing Edge Tech	●	5 sites (10%)	20 sites (40%)
Federal, Military, Academia	○	26 sites (100%)	all sites (100%)
National Labs	○	2 labs (100%)	all labs (100%)

August 11-22, 2003

CI Eastern Regional Conference

24

b7E

Assessment Worksheet: PARTNERSHIPS

BALTIMORE FIELD DIVISION ○

Criteria		Current	FY04 Target
Working Groups	○	1 on-going	1 (100%)
Task Forces	○	1 pending	1 Established (100%)
Share Strategic Information	○	On-going	Continue
Share Tactical Information	○	On-going	Continue
811 Referrals	○	On-going	Continue

August 11-22, 2003

CI Eastern Regional Conference

25

Assessment Worksheet: OPERATIONS

BALTIMORE FIELD DIVISION ○

Criteria		Current	FY04 Target
IOs Covered	○	100%	100%
Sophisticated Techniques	○	26 (100%)	100%
Aggressive Espionage Investigations, HQ Coord	○	18 (100%)	100%

August 11-22, 2003

CI Eastern Regional Conference

26

(S)

(S)

Assessment Worksheet: THREAT

BALTIMORE FIELD DIVISION ○

Criteria		Current	FY04 Target
Official Presence	○	100% covered	100%
Unofficial Presence	○	100% of known presence	100%
Unofficial Temporary Status	○	100% of known presence	100%
Report Intel Activities against WMDs & CNIAs	○	100% covered	100%

August 11-22, 2003

CI Eastern Regional Conference

27

b1
b7E

~~SECRET~~

~~SECRET~~

Assessment Worksheet: POLICYMAKERS

BALTIMORE FIELD DIVISION

Criteria		Current	FY04 Target
Policy Obstacles Referred to HQ	☐	0%	100%
Briefings to Official Visitors	☐	100%	100%

August 22-23, 2003

CI Eastern Regional Conference

28

Enabling Strats: Workforce Expertise

- Training
- Experience
- Continuity

August 22-23, 2003

CI Eastern Regional Conference

29

Workforce Expertise: Training

BALTIMORE FIELD DIVISION

Agents with 6 or more years in the program (9 SAs) should have completed 80% of the following:

- Basic 4 week course
- Cultural
- Area specific
- Country operations
- Language

Assessment	Current	'04 Targets
☐	2 SAs / 20%	50%

August 22-23, 2003

CI Eastern Regional Conference

30

Workforce Expertise: Experience

BALTIMORE FIELD DIVISION

Field Office Experience:

- Field SSAs have a minimum of 5 years FCI experience (2 SAs)
- SSAs in establishment offices must have at least 3 years specific program experience (N/A)

Assessment	Current	'04 Targets
☐	2 SSAs / 100%	100%

August 22-23, 2003

CI Eastern Regional Conference

31

Enabling Strats: Resource Management

- CI Squads
- Funding/staffing levels
- Adequate Equipment

August 22-23, 2003

CI Eastern Regional Conference

32

Resource Management: Staffing

BALTIMORE FIELD DIVISION

Field Office Staffing:

- Field office maintains 80% of identified staffing requirements (20 FLS)
- Field office maintains 5:1 ratio of agents to analysts (3 analysts)

Assessment	Current	'04 Targets
☐	7:1 ratio	5:1 ratio

August 22-23, 2003

CI Eastern Regional Conference

33

Resource Management: Equipment

BALTIMORE FIELD DIVISION

Field office has:

- SCIF or access to a SCIF
- Secure computers
- Secure communication capabilities

Assessment	Current	'04 Targets
☐	100%	100%

August 22-23, 2003

CI Eastern Regional Conference

34

Enabling Strats: Intelligence

- Collection Requirements
- Asset Base
- IT Systems
- Intelligence Products

August 22-23, 2003

CI Eastern Regional Conference

35

Intelligence: Collection

Baltimore Field Division

Field office is providing:

- Full response to all collection requirements
- Submit IIRs, other reports on relevant information collected

Assessment	Current	'04 Targets
☐	100% (60)	100%

August 22-23, 2003

CI Eastern Regional Conference

36

~~SECRET~~

~~SECRET~~

Intelligence: Asset Management		
<i>Baltimore Field Division</i>		
Field Offices ensure that		
-- All assets have been validated		
-- Asset information meets national information requirements		
Assessment	Current	'04 Targets
☐	All but one Asset	100%

August 21-22, 2003 CI Eastern Regional Conference 37

Baltimore Field Division	
Summary Report	
Overall: ☐ Making progress toward meet Program Objectives	
<u>Program Strategy</u>	<u>Enabling Strategies</u>
☒ Domain	☐ Workforce
☐ Partnerships	☐ Resources
☐ Operations	☐ Intelligence
☐ Threat	
☐ Policy-makers	

August 21-22, 2003 CI Eastern Regional Conference 38

~~SECRET~~

Serial Description ~ Unrecorded Serial

b7C,
b7C,

b7E

b7E

b7C, b7E

b7C, b7E
b7C, b7E
b7E
b7E
b7C, b7E
b7E
b7C, b7E

No Duplicate Pages
FBI040964