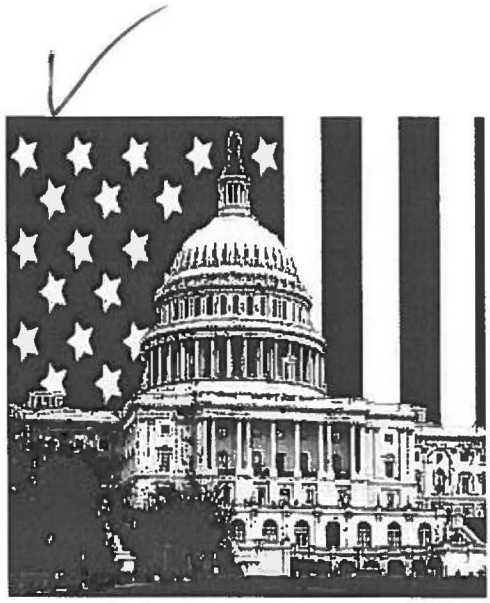
"Welcome to GGSG-Eng!"



Global Government Solutions Group - Eng

New Hire Welcome Page

- Part 1 -

We are exceptionally glad to have you joining us as part of the GGSG-Eng Team today. We value you, and your ideas, as an individual in our organization. We are looking forward to working with you and to the contributions that you will make to our projects, to our mutual enjoyment of a fun place to work, and to Cisco's performance in the marketplace. From all of us already in the Team.....Welcome aboard!

This page is designed to help you get oriented in your new position by guiding you through some of the steps and processes that you will need to take to get started here. Some steps are general to Cisco and apply to all Cisco new-hires. Other steps are particular to GGSG-Eng and the security policies that we must adhere to in serving our Government customer with sensitive information. The goal of this "**Part 1**" page is to provide you with a "one stop shopping" resource of pointers to all of those resources for getting your laptop, cube, accounts, and etcetera ready to begin business. Please work your way down the page for information and actions.

Once you are complete here, go on to **Part 2**, which will introduce you to some details of our Organization & Culture, our Project Activities, and our Information Security boundaries and approaches. A link is provided at the bottom of this page.

**** Please provide feedback to improve this page, or news on out of date pointers, to John Morris. ****

If you need assistance with any items along the way, please contact the following:				
Earlene Wiggins Admin on 2nd floor 392-3909	Your new manager or mentor - -	John Morris Mgmt Team New Hire process oversight 392-7203	HR Connection San Jose Corporate office (408) 526-5999	

Cisco New Hire Dashboard

- New Hire Checklist - Enroll in benefits, enroll in stock plans, complete initial 3-month performance review
- 90-Day Plan - All employees new to Cisco (external hires) need to fill out one of these forms to review with your manager
- Starting at Cisco - Synchronize passwords, order business cards, learn Cisco's telecommuting policies
- Training and Development - Learn about available classes and training opportunities
- ISO Video and Assessment - As part of the ISO process **ALL** employees who join GGSG-Eng are

required to take the BMS Engineering training class and assessment.

Office Supplies

- Please help yourself to the general office supplies provided by Cisco in the Mail Room on the center aisle of each floor in Cisco buildings
- If you have a need for something not provided in the Mail Room, please see Deb Smith for special ordering

Laptop

- **Acquisition** - All Cisco Engineering employees are provided with a laptop by Cisco. Chances are, Earlene has yours waiting at her place.
- **Standard Software** - New laptops come to us through an IT group that pre-installs a standard Cisco image of Operating System and Applications. If your laptop did not come pre-installed or has problems at initial boot up, you may find information or open a case with Internal Technical Support for Desktop Computing.
- **Additional Software** - To install additional software when necessary, you may find the installation stubs at SoftTracker. Many standard applications are site-licensed and may be installed at no charge to the department. For applications with a charge, it is best to speak with your manager first.
- **Backup Protection** - GGSG-Eng uses a different backup system than the rest of Cisco in order to restrict access to sensitive information on GGSG-Eng laptops and PC's. **Do not install the Cisco Corporate backup system from SoftTracker (Connected TLM).** Instead, please install the back up system from GGSG IT at Secure Connected TLM Backup Install Guide.
- **Hard Drive Protection** - All members of GGSG, of which GGSG-Eng is a part, are required to install PointSec to encrypt hard drive data and protect the information if the laptop is lost or stolen. Please install it from the GGSG IT page at PointSec Install Guide.
- **Message Protection** - If you transmit sensitive messages with restricted or controlled information, but not government "classified" information, you must also install Pretty Good Privacy (PGP) from the GGSG IT page at the PGP Install Guide.
- **Laptop Accessories** - An accessory package is normally pre-stocked and provided by Deb on your start day. Please see Earlene for the package which includes Monitor, Keyboard, Mouse, Spare battery, AC Adaptor, Security Lock, and Carry Case.

Other Equipment

- **Sun Workstation** - Please see your manager and mentor to determine if a Sun Workstation should be ordered based on your project and position. Some projects are classified and all workstations are inside of secure lab spaces. Deb normally places the orders after receiving a request from a manager.
- **IP Phone** - The desktop IP Phones are normally provided and on the desk prior to your arrival. If you do not have one in your cube/office, please see Earlene for assistance.
- **Cube Accessories** - Other accessories and work-helps to go in cubes are normally pre-stocked by Earlene in her supply closet. Please see Earlene if you need a Whiteboard, Coat-hangar, File-folder Organizer, or other such equipment. Whiteboard pens, erasers, and cleaning fluid are available in the Mail Room supply locker.

Accounts and Services

- **Phone and Voicemail Account** - The Internal Technical Support team should have already taken care to establish and setup your accounts prior to your start date. If there is a problem, you may find

information or open a case with them.

- **Meeting Maker Account** - The I.T. Access Team should have already established and setup your Meeting Maker Account prior to your start date. If there is a problem with the account they set up, you may find information or open a case with them. If there is no account set up and you need to initiate one, then go to OnRamp.
- **Cube Nameplate** - There should be a name plate with your name and a Cisco logo in your cube name plate holder. If not, please see Deb for assistance.
- **Mailbox** - A mailbox or folder, labeled with your name, should already be provided in the Mail Room on the floor where your cube resides. If not, please see Earlene for assistance.
- **Lab Access** - In order to gain access to the GGSG-Eng 2nd Floor general laboratory facilities, you must complete the three steps listed below. For special project laboratory facilities (e.g. classified projects) there is an additional requirement of being added to that project access list.
  1. Complete ESD Training
  2. Complete Lab Safety Training (SABSCIS001ENG)
  3. When complete with ESD and Lab Safety, go to the Lab Access link to open a case to gain access. The case will be forwarded to David Heuser with information on completion of training and floor access.

Welcome Aboard!

*** Go to GGSG-Eng New Hire Orientation Part 2

"Welcome to GGSG-Eng!"

Global Government Systems Group - Engineering

New Hire Welcome Page

- Part 2 -

Welcome to **Part 2** of the GGSG-Eng New Hire Orientation site. The **Part 1** web page should have helped you to set up your laptop, cube equipment, and service accounts so that you are all ready to begin settling down to business. The objective of this page is to help familiarize you to some details of our GGSG-Eng Organization & Culture, our Project Activities, and our Information Security boundaries and approaches. It is presented in a Question and Answer format, so that you may gain answers in a few minutes of reading, to benefit from hours of lessons learned from your team mates ahead of you, as we have wrestled with the same questions. We are glad to have you aboard with us!

**** Please provide feedback to improve this page, or news on out of date pointers, to John Morris. ****

ORGANIZATION & CULTURE **PROJECT ACTIVITIES** **INFORMATION SECURITY**

GGSG-Eng ORGANIZATION & CULTURE

What is our GGSG-Eng Mission or Charter? The charter of the GGSG-Eng is to enhance Cisco's business revenue from and support to government agencies, as the arm of Cisco specifically tailored to government-unique requirements, focused upon but not limited to, the ability to work in classified and ITAR environments. The details of our mission is further broken down into the following three areas:

1. **Address Government Unique Requirements**
   - Extend existing and develop new products for government-specific use.
   - Provide specialized marketing and dev resources that can operate in classified environments.
   - Ensure Cisco complies with government-specific policies and regulations (ITAR, firewall, security).
2. **Provide Analysis and Guidance**
   - Define government strategic and tactical product and solution direction.
   - Analyze new opportunities and prioritize projects.
   - Educate and advise Cisco on government specific requirements.
3. **Collaborate Internally and Externally**
   - Partner globally with Cisco Sales, CDO, Tech Center, BUs, & Central Marketing Organization.
   - Facilitate interaction between Cisco BUs and System Integrators/ Government Customers.

What is our GGSG-Eng culture? The goal of the GGSG-Eng Team is to establish a culture

like some might call "old Cisco". Some of the highlights of the environment we work in here are open communication, friendliness, disciplined adherence to process for the sake of "doing the right thing" and "good scholastic Engineering methodology", but not process merely for process' sake. We are building a crisp professional team here that runs on track and on schedule, but we have fun and enjoy working together while we do that. We take care of each other. We treat others as we desire to be treated ourselves. GGSG-Eng Culture means having named team members on board and allocated prior to Execute Committing a project, and not committing to a project and schedule based on "To Be Hired" positions. We will hold firmly to an appropriate ratio of developers to testers on software development projects, which will not exceed 2:1. We plan together, we work together, we celebrate together. These are some of the principles that form the culture that we have created and desire to maintain here in the Government Systems Unit.

How is GGSG Organized and what are the other parts? The Global Government Solutions Group (GGSG) is focused on supporting global governments by delivering enhanced mission capabilities through thought leadership, innovation and transformation. GGSG is cohesively linked and integrated with the Corporate Strategic Security Programs (CSSP) group. The mission of Cisco's Corporate Strategic Security Program encompasses a broad spectrum of security issues including - Information Security, Security Certifications and Critical Infrastructure and Asset Protection. A full listing of GGSG-Eng and the other sub-components of GGSG/CSSP is available at the GGSG/CSSP web site.

Where does GGSG-Eng fit into GGSG? GGSG-Eng is the "Custom Engineering" unit of the Global Government Solutions Group (GGSG), which includes a Marketing Team, an Engineering Team, a Finance Team, and a small Customer Support Engineering Team for some special products where we provide support in place of TAC. You can find the Cisco Corporate objectives and information about GGSG-Eng at the GGSG-Eng Cisco Employee Connection web page. In the past, the Federal Sales Team and Federal Support Programs team sold and supported standard Cisco products from non-government-specific BU's throughout Cisco to the governments of the US and others around the world. A need for customized software and hardware products precipitated the creation of the GGSG-Eng wing of GGSG. GGSG-Eng is focused on addressing governments' unique requirements by leveraging and extending Cisco's core products and technologies, developing new product lines, and engaging with system integrators to meet government program-specific requirements.

Why is GGSG-Eng outside of CDO? There are likely several good reasons that top management of Cisco Systems chose to establish GGSG-Eng separated from the massive Cisco Development Organization, where all other Engineering BU's are located. One primary reason is the separation of an engineering division that can register with the government as a separate agency from CDO for programs that involve controlled government information, either due to its classified or sensitive nature and handling requirements, or due to International Traffic in Arms Regulations (ITAR). Some of the products GGSG-Eng is creating are ITAR-controlled, and GGSG-Eng is the only organization in Cisco that is ITAR Registered for this special government work. It is much easier to have a small team like GGSG-Eng conform to government standards for security and ITAR, which has an added overhead cost to support, than to go to the effort and expense to certify all of CDO for these programs. See more information on ITAR below under GGSG-Eng INFORMATION SECURITY.

What are the roles of Program Managers and First Line Managers in GGSG-Eng? GGSG-Eng has a Program Manager (PM) assigned to all Engineering projects, because we work in a mode and environment where the value added by our Program Management team is critical. PMs typically do not have direct reports to them. First Line Managers have direct reports for teams of Software Development, Hardware Development, and Software Test. Other infrastructure headcount such as Documentation, Tools Development, and such are included in those teams also.

Program Manager responsibilities include:

- Guiding projects through entire development cycle from requirements and specifications development, through product fielding and support.
- Liaison and coordination of all teams involved in the project to accomplish on-time results of project deliverables.
- Development and maintenance of the Project Plan document, that serves as the plan-of-record or project-roadmap for all team members to work towards.
- Tracking and reporting on project status at weekly Engineering Operations Review meetings.

First Line Manager responsibilities include:

- Guidance and oversight of technical project sub-teams that exist within their larger team (Development, Test, Hardware, etc.)
- Administrative watch care and support of the careers of the direct reports within their teams for areas such as annual focal reviews, stock, bonus, promotion, time off, training classes, and other human resource issues.
- Assembly, compilation, review and submission of quarterly budgets.
- Team building, recruiting, morale, and headcount to project assignments.

What is the Career Navigator and how does GGSG-Eng make use of it? The Career Navigator Tool is a collection of information useful to both contributors and managers for long term career development. It details in bulleted form the information for Job Responsibilities, Critical Success Factors, and Long Term Career Development Planning for each role, and in each grade. GGSG-Eng makes use of this information in setting a level expectation for rankings and ratings of how each of us has performed across the entire organization, and that information is used in determinations for things like stock and bonus distributions, and promotions. The GGSG-Eng Career Navigator Tools are available at the following links:

- GGSG-Eng Software Development Career Navigator
- GGSG-Eng Software DevTest Career Navigator
- GGSG-Eng Hardware Development Career Navigator

GGSG-Eng PROJECT ACTIVITIES

In overview, what are the current and future projects that GGSG-Eng is working on? There are several exciting engineering projects currently underway in the Global Government Solutions Group - Engineering, and many more on the roadmap ahead of us, as factors like resources available, business case, and time to market requirements raise them to the top of our priority list. The governments that we serve as our customers have need for customized or certified networking products across the entire spectrum of data, voice, security, network management, etc., so GGSG-Eng's projects cover a wide spectrum of product areas. For a listing of projects, an executive summary statement, and pointers to detailed documents on each project, look in the left hand column on this web page, select Engineering OPs, and then select the project name (eg. Valiant) under each of the five "bucket" tabs. More about these buckets in a few questions further down this page.

How does GGSG-Eng engage with GGSG-Marketing, and vice versa? The Global Government Systems Group - Engineering operates under the common high-disciplines associated with a professionally experienced product development and engineering business

unit. Marketing drives Engineering through detailed and objective development of product requirements, time to market requirements for such products, and the associated business cases for such products. Together, the GGSG-Eng Management Team analyzes this information to develop our future task lists with associated payoffs in terms of forecast business revenue, and compares that to available appropriately skilled resources or availability to gain new resources, in order to determine our Development Priority List and forecast schedule of what projects we will take up next. This collection of information and the process of its documentation, presentation, analysis, and decision making results are defined in the Cisco Great Engineering Methodology (GEM) process, to which we adhere (see GEM/Templates on left hand column). GEM defines the stages of the process development cycle, as well as the agents or departments responsible for each stage.

How do we know or select what projects GGSG Engineering will take up next? There are many potential projects on our radar horizon that have either been brought to GGSG-Eng by another BU or marketing organization, or brought in by our own team within the Global Government Systems Group - Engineering or the GGSG Group. GGSG-Eng does not have the necessary resources to execute every project on the wish list immediately in parallel. Therefore, we have established a process to prioritize and sequence the execution of projects in accordance with our charter business goals. From an earlier question you have now seen the five "buckets" that categorize the projects on our docket. From our GGSG-Eng business strategy we have target numbers for the percentage of our total resources that we desire to allocate to each of those buckets. The following lists the buckets and the resource allocation targets for each:

- Non-Terrestrial - Product development efforts directly related to putting Cisco routing into outer space
- DoD Voice - Projects where GGSG-Eng applies resources to add features / provide additional testing to VTG's and MCEBU's products to enhance VoIP sales to government communities.
- Tactical Mobility - Projects where GGSG-Eng is engaged with integrators in solving mobile ad hoc networking problems.
- General Goverment - Projects that are generic in nature such as setting up the Government Automated Regression Facility.
- DISA Network - Projects directly related to helping the Defense Information Systems Agency solve their network problems. This includes special testing of images prior to deployment or testing of hardware/software combinations prior to purchase decisions.
- Contracted Federal - Projects related to potential development which requires Cisco to work in areas not open to the general company.

Each month a group of individuals from Marketing, Finance and Engineering meet for the Opportunity Assessment Review (OAR) where new opportunities for potential revenue-earning projects are reviewed for business case, time to market constraints, national urgency concerns, engineering resources required, time estimated for completion, and other metrics. Each opportunity is categorized into its appropriate bucket, and is prioritized for sequence of future engagement on that bucket's Development Priority List (DPL). There is a DPL maintained for each bucket, which is visible to managers from a link off of the GGSG-Eng web page. Another web tool off of the Manager's link keeps track of real-time allocation of resources within each bucket relative to the targets (eg. 50%) above. This tool is referred to as the Engineering Bucket Allocation Process, or ENGBAP, and the management team uses this, and other GGSG management tools, to manage and plan to our GGSG-Eng business strategy; continuously striving together towards our common goals with a common picture.

How does GGSG-Eng interact and engage with other Business Units within Cisco? GGSG-Eng interacts and engages with other BU's within Cisco in the best way that we can see to impact and improve Cisco's corporate bottom line for the shareholders. There are many BU's that have products that global governments may desire to procure, and we ourselves are simply one of those BU's. We target 50% of our engineering development and test efforts towards GGSG-Eng products that affect our own BU's profit & loss, and the other 50% is applied on projects either inside or outside our BU where our government-specific knowledge, expertise, or relationships may be leveraged from within our team to enhance government sales opportunities for those products.

What are GGSG Engineering's goals and initiatives? The GGSG Engineering management team routinely sets goals and initiatives for our organization for the next six months on the road ahead of us. Here is a brief history of our high-level organizational goals:

September - February 2005

1. EC HAIPE Engineering Strategy in Mid-October 2004
    - Blacksky, Spumoni, Gelato
2. EC Space Engineering Strategy
    - Flipper, Aqueduct
3. EC DoD Voice Engineering Strategy
    - Batphone PBX1, Batphone IP STE, Riddler, Griphus, Call Manager, Future PBX certification plans
4. EC DISA Network Support Strategy
5. Execution on GARF
    - GARF-Raven on beta Jan 2005, on r1.0 March 2005
6. Execution on Raven
7. Refine strategy for NTA development, support, delivery, and drive to next release EC
8. Evaluate Engineering resource assignments quarterly

March - August 2004

1. Execute, execute, execute on current projects
2. Complete build out of the Engineering team based on Sep 03 planning, and establish and execute next phase of the organization's growth
3. Refine engineering processes and tools
4. Establish understanding of government requirements and processes for hardware and software development
5. Establish "team cohesiveness"
6. Establish Human Resources and Hiring process maturity

September 2003 - February 2004

1. Establish engineering processes and tools
2. Focus and plan future execution priorities
3. Execute efficiently
4. Build organizational infrastructure and fill in the team
5. Mature internal HR processes
6. Become a team

June - August 2003

1. Build initial team quickly -- "30 hires in 30 days"
2. Gain measurable results and impact
3. Pursue learning and education
4. Pick a few long-term bets

GGSG-Eng INFORMATION SECURITY

When do I apply for a security clearance and how do I apply? Security clearances are only given when required for a particular project's work, and in general, the US Government strives to minimize the number of clearances that exists at any given time. When your project work does require access to classified information at some point, which could be right away or never at all, either the the project's Program Manager or your First Line Manager will ask you to begin the process of application for the appropriate level of clearance. The first step in applying for a clearance is to go to the Government Security Office (GSO) web site and under the TOOLS heading on the right, select PERSONNEL CLEARANCE REQUEST to get to the SF-86 form to fill out and submit back to GSO.

What is ITAR and how does it impact or affect us? The United States Government controls the development, production, export, and procurement of weapons and armories within and through the international borders of the US and its territories by the laws and regulations called International Traffic in Arms Regulations, or "ITAR". Jurisdiction for management of these policies falls within the State Department, and you may find the entire collection of their information at the State Department ITAR web site. For companies or agencies within the US to handle, develop, sell, (etc.) equipment and materials that fall within the definitions of ITAR-controlled devices, technologies, or substances, they must be officially approved and registered to do so by the State Department. GGSG-Eng is ITAR approved and registered as an agency outside of the Cisco Development Organization (CDO). Obtaining that certification was no small undertaking. CDO, as a whole, is not ITAR approved and registered, so other BU's or organizations within Cisco cannot work with ITAR-controlled devices, by Federal law.

A wealth of organized information about the details of ITAR, and the specifics that impact our decision making on our projects, has been collected at the GGSG-Eng ITAR web site. We all need to be aware of the basic criteria that make something ITAR-controlled or not, and that information is available there at the ITAR Red Flags & FAQs link. Please take a moment to peruse this document and familiarize yourself with ITAR information.

What are the levels of classification of information and what do they mean? Classified information falls into several different levels of classification, depending primarily upon the degree of potential harm that could result to the United States Government, its resources, or its allies, from losing control of that information and it falling into the hands of our adversaries. Each level of classification has defined access, handling, and storage procedures associated with it. You have heard a brief description of these levels and controls during your Security In-Briefing with Pete Plezia or Greg Bolick. Some categories of classified information include, for example, CONFIDENTIAL, SECRET, or TOP SECRET. Sub-categories also exist within those nomenclatures such as Special Access Programs (SAP) or Sensitive Controlled Information (SCI). The details about how to properly access, label, handle, store and transport these types of information is briefed to individuals cleared for that information at the time of receiving the clearance. Handling and storage information is not released to non-cleared individuals.

If you ever see classified information of any form lying out in the open with no one around it (uncontrolled), you must take steps to safeguard the information immediately. Either stay with/near the documents for a moment to see if the owner returns, or collect the documents (without perusing them) and take them to Pete or Greg. Notify Pete or Greg of any incidents like this for proper follow up and correction to our procedures or training.

There are also a few categories of unclassified but sensitive information that will exist in the GSU work environment. Some documents may be marked UNCLASSIFIED, SENSITIVE, or FOR OFFICIAL USE ONLY (FOUO), and these working papers should be kept secure in locking cabinets or drawers when ever they are not in use.

How are we going to store and access sensitive or classified documents? Surely we can't use EDCS. Classified documents must be handled and stored according to the policies described in the paragraph above. EDCS cannot be used to store any classified material whatsoever. This is an area where GGSG Engineering must find other solutions unique from the rest of Cisco. Unclassified but sensitive project documents will generally not be stored on EDCS either, and instead, a local GGSG-Eng Server within the access-controlled environment (2nd floor) may be used for electronic storage of files and documents.

How are we going to log and track software defects for sensitive or classified projects? Surely we can't use DDTS. For classified and/or sensitive projects, defect tracking will also require an alternate solution from the normal Cisco corporate tool of Distributed Defect Tracking System (DDTS). Bug reports for classified or sensitive projects, or perhaps ITAR-controlled versions of IOS, may contain information not releasable to individuals not cleared or outside of GGSG-Eng. Therefore, an alternate bug tracking software database tool is under investigation now, and will be installed within the access-controlled environment and perhaps within the lab room dedicated for very sensitive projects.

How are Developers going to maintain builds, and Testers going to maintain scripts for sensitive or classified projects? Surely we can't use Cisco corporate VOBs. Storage of software build files and test scripts for classified or sensitive projects must also be unique for GGSG Engineering, in accordance with the controls for that information described above. The Information Technology (IT) staff that support GGSG-Eng are investigating and planning today, how to install and support a secure development, build, storage, and test environment to support the requirements for classified software projects.

How are we going to use our laptops and PC's for sensitive and classified project work, since corporate IT staff can still "logon" to our machines? This is a current and legitimate concern that is still under investigation by our GGSG-Eng IT team for a viable and cost-effective solution. Currently, the corporate IT staff do, in fact, have the ability to remotely connect to our laptops and PC's while on the Cisco network and see or copy files and documents. Plans are well underway to resolve this problem. As an interim means, PGP may be used to encrypt and secure individual files to protect sensitive information and documents. Please use precautions to ensure PGP pass-phrases are not lost, which could result in the loss of the file and the work to create it, since no one could access it without the pass-phrase.

THANK YOU FOR TAKING THE TIME TO READ ALL OF THIS INFORMATION, AND WELCOME TO GGSG-Eng!! :-)