

Exhibit 300: Capital Asset Plan and Business Case Summary**Part I: Summary Information And Justification (All Capital Assets)****Section A: Overview (All Capital Assets)**

1. Date of Submission: 8/24/2007
2. Agency: Department of Transportation
3. Bureau: National Highway Traffic Safety Administration
4. Name of this Capital Asset: NHTSA020: Artemis
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.) 021-18-01-14-01-1170-00
6. What kind of investment will this be in FY2009? (Please NOTE: Investments moving to O&M in FY2009, with Planning/Acquisition activities prior to FY2009 should not select O&M. These investments should indicate their current status.) Mixed Life Cycle
7. What was the first budget year this investment was submitted to OMB? FY2001 or earlier
8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap:
- Artemis is a mission-critical system that directly supports NHTSA in its mission to reduce fatalities, injuries and economic loss resulting from traffic crashes. Artemis provides an efficient means to identify serious safety defects early in the vehicle equipment and component production cycle and influences safety recalls promoting a safer environment for drivers and passengers across the nation. Artemis provides secure collection and centralized storage of critical safety information, including imaging and document management capabilities, data analysis tools, and a public website for information dissemination and consumer data collection in accordance with E-gov objectives. Artemis is essential to meet legislative requirements enacted in 2000 called The Transportation Recall Enhancement, Accountability and Documentation (or TREAD) Act. The law increases consumer safety through mandates assigned to NHTSA. It was drafted in response to fatalities related to vehicle crashes, and was influenced by manufacturers of vehicles, tires, child safety seats, and equipment, as well as consumer safety advocates. During initial development, NHTSA conducted an alternatives analysis in 2001 and determined that Artemis was the best suited solution to meet the following major components of the TREAD Act: 1) Requires that vehicle manufacturers report to the National Highway & Transportation Safety Administration (NHTSA) when they conduct a safety recall or other safety campaign in a foreign country; 2) Require that vehicle manufacturers report information related to defects, reports of injury or death related to its products, as well as other relevant data in order to comply with "Early Warning" requirements; 3) Require that NHTSA have the ability to report non-compliance when a vehicle manufacturer intentionally violates the new reporting requirements when a safety-related defect has subsequently caused death or serious bodily injury. In order to satisfy the requirements of 49 CFR Part 579 (Early Warning), over 700 manufacturers of motor vehicles, tires, child safety seats, and motor vehicle equipment, submit quarterly reports to NHTSA via Artemis and its secure FTP servers. Without Artemis, there would be no reasonable alternative to collect and analyze the huge volumes of data received. Approximately 275 internal users access Artemis via secure INTRANET and there are over 9,500 unique visitors of the public website each day.
9. Did the Agency's Executive/Investment Committee approve this request? Yes
- a. If "yes," what was the date of this approval? 8/24/2007
10. Did the Project Manager review this Exhibit? Yes
11. Contact information of Project Manager?
- Name: Borris, Frank
- Phone Number: Redacted
- Email: frank.borris@dot.gov
- a. What is the current FAC-P/PM certification level of the project/program manager? Mid/Journeyman-level
12. Has the agency developed and/or promoted cost effective, energy-efficient and environmentally sustainable techniques or practices for this project? Yes
- a. Will this investment include electronic assets (including computers)? Yes

- b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only) No
1. If "yes," is an ESPC or UESC being used to help fund this investment?
 2. If "yes," will this investment meet sustainable design principles?
 3. If "yes," is it designed to be 30% more energy efficient than relevant code?
13. Does this investment directly support one of the PMA initiatives? Yes
- If "yes," check all that apply: Expanded E-Government
- a. Briefly and specifically describe for each selected how this asset directly supports the identified initiative(s)? (e.g. If E-Gov is selected, is it an approved shared service provider or the managing partner?) Artemis supports the objectives of the E-Government Act of 2002 by using internet-based technology to enhance citizen access to government information. Over 9,500 unique visitors each day use Artemis to search and browse safety information in the form of recalls, investigations, consumer complaints and technical service bulletins. Citizens use this information to make wiser decisions about vehicle and equipment operation or buying. Over 45,000 citizens also use Artemis to report defects.
14. Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit www.whitehouse.gov/omb/part.) Yes
- a. If "yes," does this investment address a weakness found during a PART review? No
 - b. If "yes," what is the name of the PARTed program? NHTSA Operations and Research
 - c. If "yes," what rating did the PART receive? Moderately Effective
15. Is this investment for information technology? Yes
- If the answer to Question 15 is "Yes," complete questions 16-23 below. If the answer is "No," do not answer questions 16-23.
- For information technology investments only:
16. What is the level of the IT Project? (per CIO Council PM Guidance) Level 2
17. What project management qualifications does the Project Manager have? (per CIO Council PM Guidance) (1) Project manager has been validated as qualified for this investment
18. Is this investment or any project(s) within this investment identified as "high risk" on the Q4 - FY 2007 agency high risk report (per OMB Memorandum M-05-23) No
19. Is this a financial management system? No
- a. If "yes," does this investment address a FFMI compliance area?
 1. If "yes," which compliance area:
 2. If "no," what does it address?
 - b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52
20. What is the percentage breakout for the total FY2009 funding request for the following? (This should total 100%)
- | | |
|----------|-----------|
| Hardware | 2.000000 |
| Software | 8.000000 |
| Services | 90.000000 |
| Other | 0.000000 |
21. If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities? Yes
22. Contact information of individual responsible for privacy related questions:

Name Smith, Delores M
 Phone Number Redacted
 Title Information Systems Security Officer (ISSO)
 E-mail dee.smith@dot.gov

23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval? Yes

Question 24 must be answered by all Investments:

24. Does this investment directly support one of the GAO High Risk Areas? No

Section B: Summary of Spending (All Capital Assets)

1. Provide the total estimated life-cycle cost for this investment by completing the following table. All amounts represent budget authority in millions, and are rounded to three decimal places. Federal personnel costs should be included only in the row designated "Government FTE Cost," and should be excluded from the amounts shown for "Planning," "Full Acquisition," and "Operation/Maintenance." The "TOTAL" estimated annual cost of the investment is the sum of costs for "Planning," "Full Acquisition," and "Operation/Maintenance." For Federal buildings and facilities, life-cycle costs should include long term energy, environmental, decommissioning, and/or restoration costs. The costs associated with the entire life-cycle of the investment should be included in this report.

Table 1: SUMMARY OF SPENDING FOR PROJECT PHASES (REPORTED IN MILLIONS)									
(Estimates for BY+1 and beyond are for planning purposes only and do not represent budget decisions)									
	PY-1 and earlier	PY 2007	CY 2008	BY 2009	BY+1 2010	BY+2 2011	BY+3 2012	BY+4 and beyond	Total
Planning:	0.5	0.1	0	0.02	Redacted	Redacted	Redacted	Redacted	Redacted
Acquisition:	9.816	0.4	0	0.2	Redacted	Redacted	Redacted	Redacted	Redacted
Subtotal Planning & Acquisition:	10.316	0.5	0	0.22	Redacted	Redacted	Redacted	Redacted	Redacted
Operations & Maintenance:	9.633	2.08	2.163	2.25	Redacted	Redacted	Redacted	Redacted	Redacted
TOTAL:	19.949	2.58	2.163	2.47	Redacted	Redacted	Redacted	Redacted	Redacted
Government FTE Costs should not be included in the amounts provided above.									
Government FTE Costs	0.776	0.143	0.147	0.152	Redacted	Redacted	Redacted	Redacted	Redacted
Number of FTE represented by Costs:	5	1	1	1	Redacted	Redacted	Redacted	Redacted	Redacted

Note: For the multi-agency investments, this table should include all funding (both managing partner and partner agencies). Government FTE Costs should not be included as part of the TOTAL represented.

2. Will this project require the agency to hire additional FTE's? No

a. If "yes," How many and in what year?

3. If the summary of spending has changed from the FY2008 President's budget request, briefly explain those changes:
 Redacted

Section C: Acquisition/Contract Strategy (All Capital Assets)

1. Complete the table for all (including all non-Federal) contracts and/or task orders currently in place or planned for this investment. Total Value should include all option years for each contract. Contracts and/or task orders completed do not need to be included.

Exhibit 300: NHTSA020: Artemis (Revision 13)

Contracts/Task Orders Table:																* Costs in millions
Contract or Task Order Number	Type of Contract/ Task Order	Has the contract been awarded (Y/N)	If so what is the date of the award? If not, what is the planned award date?	Start date of Contract/ Task Order	End date of Contract/ Task Order	Total Value of Contract/ Task Order (\$M)	Is this an Interagency Acquisition ? (Y/N)	Is it performance based? (Y/N)	Competitively awarded? (Y/N)	What, if any, alternative financing option is being used? (ESPC, UESC, EUL, N/A)	Is EVM in the contract? (Y/N)	Does the contract include the required security & privacy clauses? (Y/N)	Name of CO	CO Contact information (phone/email)	Contracting Officer Certification Level (Level 1,2,3,N/A)	If N/A, has the agency determined the CO assigned has the competencies and skills necessary to support this acquisition ? (Y/N)
Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted
Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted

2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:

3. Do the contracts ensure Section 508 compliance?

Yes

a. Explain why:

To ensure compliance with Section 508 of the Rehabilitation Act of 1973, NHTSA includes in its contracts and agreements the following language: "All deliverables and services rendered under this contract/agreement must comply with the accessibility standards at 36 CFR 1194." For example, Artemis contractors are required to ensure that HTML code contains "alt" attributes for accessing web-based data and information and that user documentation, manuals and online help files are available.

4. Is there an acquisition plan which has been approved in accordance with agency requirements?

No

a. If "yes," what is the date?

b. If "no," will an acquisition plan be developed?

Yes

1. If "no," briefly explain why:

Section D: Performance Information (All Capital Assets)

In order to successfully address this area of the exhibit 300, performance goals must be provided for the agency and be linked to the annual performance plan. The investment must discuss the agency's mission and strategic goals, and performance measures (indicators) must be provided. These goals need to map to the gap in the agency's strategic goals and objectives this investment is designed to fill. They are the internal and external performance benefits this investment is expected to deliver to the agency (e.g., improve efficiency by 60 percent, increase citizen participation by 300 percent a year to achieve an overall citizen participation rate of 75 percent by FY 2xxx, etc.). The goals must be clearly measurable investment outcomes, and if applicable, investment outputs. They do not include the completion date of the module, milestones, or investment, or general goals, such as, significant, better, improved that do not have a quantitative or qualitative measure.

Agencies must use the following table to report performance goals and measures for the major investment and use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Map all Measurement Indicators to the corresponding "Measurement Area" and "Measurement Grouping" identified in the PRM. There should be at least one Measurement Indicator for each of the four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov. The table can be extended to include performance measures for years beyond FY 2009.

Performance Information Table								
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
2007	Safety	Customer Results	Service Quality	Accuracy of Service or Product Delivered	Public Website Data Quality: Reduce number of duplicate and missing products from drop down menus. Proper identification of affected products is critical to NHTSA's ability to quickly identify safety defect trends.	5% of complaints received via public website contain unknown, improper, or duplicate products. This requires rework and reduces efficiency	Reduce invalid complaint products to 2.5%.	Invalid complaint products reduced to 2.1%. This result was achieved through the efforts of a dedicated data quality team.
2007	Safety	Mission and Business Results	Information and Technology Management	Information Management	The vast data collected under 49 CFR Part 579 (Early Warning Reporting) have significantly increased the quantity of safety data each investigator is required to process.	28 issues evaluated and presented per staff member per year	Increase issues evaluated by 10%	Average number of issues evaluated per staff member increased to 35 per year.
2007	Safety	Processes and Activities	Quality	Errors	Improve image quality of legacy investigation files that may have been scanned at low resolution.	A sample of 50 records indicates 8% are difficult for the average consumer to read.	Reduce number of poor quality scans to 6%.	The number of poor quality scans has been reduced to 4%.
2007	Safety	Technology	Reliability and Availability	Reliability	Decrease downtime of	5% downtime	Decrease downtime to 4%	Downtime of OCR was

Performance Information Table								
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
					optical character recognition module			reduced to zero.
2008	Safety	Customer Results	Service Accessibility	Access	Reduce customer burden when reporting alleged safety defects. This will reduce the quantity of dropped complaints and improve NHTSA's ability to identify safety defect trends.	Current online complaint form requires 5-8 minutes to complete.	Reduce average complaint submission duration by 25%.	Results will be compiled in October 2008.
2008	Safety	Mission and Business Results	Transportation	Ground Transportation	Number of potential safety issues evaluated per staff year	28 issues evaluated and presented per staff year	Increase by 15%	Results by October 2008
2008	Safety	Processes and Activities	Quality	Errors	Improve image quality of legacy investigation files that may have been scanned at low resolution.	6%	4%	Results by October 2008
2008	Safety	Technology	Efficiency	Improvement	Implement use of digital signatures on investigation and recall documents to reduce scanning burden.	There is currently no use of digital signatures.	Implement use of digital signatures on investigation resumes and recall acknowledgment letters.	Post by October 2008
2009	Safety	Customer Results	Service Accessibility	Availability	Increase availability of safety data collection by designing an implementing an online option for hispanic complainants.	The only current option for hispanic complaints is to contact the Vehicle Safety Hotline.	Implement a Spanish language online form for use by the general public and on the Vehicle Safety Hotline data entry module.	
2009	Safety	Mission and Business Results	Information and Technology Management	Information Systems Security	Use of HSPD-12 compliant technology to control role-based access.	There are no (zero) Artemis users making use of HSPD-12 compliant technology or access.	Demonstrate use of HSPD-12 compliant, role-based system access for 15 Artemis users with access to SPII and/or BCI.	
2009	Safety	Processes and Activities	Quality	Errors	Improve image quality of legacy investigation files that may have been scanned at low resolution.	4%	2%	
2009	Safety	Technology	Efficiency	Response Time	Reduce system response time for simple workflow commands.	Current document approvals average 30-60 seconds.	10-15 seconds	
2010	Safety	Customer Results	Service Accessibility	Availability	Centralized availability of complete investigation files for public access.	15% of investigation files are stored in separate databases due to differences in files structure or proprietary readers.	Reduce to 10%	
2010	Safety	Mission and Business Results	Information and Technology Management	Information Systems Security	Use of HSPD-12 compliant technology to control role-based access.	15 users	All users with access to PII	
2010	Safety	Processes and Activities	Quality	Complaints	Reduce number of complaints received by the Vehicle Safety	30 complaints/year	20 complaints/year	

Performance Information Table								
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
					Hotline concerning inability to file a complaint due to missing products.			
2010	Safety	Technology	Quality	Functionality	Options for searching recall database via the public website	There are currently 5 options for searching the recalls database. Consumers have requested more options including word searching.	Increase search options to find key words.	

Section E: Security and Privacy (IT Capital Assets only)

In order to successfully address this area of the business case, each question below must be answered at the system/application level, not at a program or agency level. Systems supporting this investment on the planning and operational systems security tables should match the systems on the privacy table below. Systems on the Operational Security Table must be included on your agency FISMA system inventory and should be easily referenced in the inventory (i.e., should use the same name or identifier).

For existing Mixed-Life Cycle investments where enhancement, development, and/or modernization is planned, include the investment in both the "Systems in Planning" table (Table 3) and the "Operational Systems" table (Table 4). Systems which are already operational, but have enhancement, development, and/or modernization activity, should be included in both Table 3 and Table 4. Table 3 should reflect the planned date for the system changes to be complete and operational, and the planned date for the associated C&A update. Table 4 should reflect the current status of the requirements listed. In this context, information contained within Table 3 should characterize what updates to testing and documentation will occur before implementing the enhancements; and Table 4 should characterize the current state of the materials associated with the existing system.

All systems listed in the two security tables should be identified in the privacy table. The list of systems in the "Name of System" column of the privacy table (Table 8) should match the systems listed in columns titled "Name of System" in the security tables (Tables 3 and 4). For the Privacy table, it is possible that there may not be a one-to-one ratio between the list of systems and the related privacy documents. For example, one PIA could cover multiple systems. If this is the case, a working link to the PIA may be listed in column (d) of the privacy table more than once (for each system covered by the PIA).

The questions asking whether there is a PIA which covers the system and whether a SORN is required for the system are discrete from the narrative fields. The narrative column provides an opportunity for free text explanation why a working link is not provided. For example, a SORN may be required for the system, but the system is not yet operational. In this circumstance, answer "yes" for column (e) and in the narrative in column (f), explain that because the system is not operational the SORN is not yet required to be published.

Please respond to the questions below and verify the system owner took the following actions:

1. Have the IT security costs for the system(s) been identified Yes
and integrated into the overall costs of the investment:
 a. If "yes," provide the "Percentage IT Security" for the 18.00
budget year:
2. Is identifying and assessing security and privacy risks a part Yes
of the overall risk management effort for each system
supporting or part of this investment.

3. Systems in Planning and Undergoing Enhancement(s), Development, and/or Modernization - Security Table(s):			
Name of System	Agency/ or Contractor Operated System?	Planned Operational Date	Date of Planned C&A update (for existing mixed life cycle systems) or Planned Completion Date (for new systems)
Redacted	Redacted	Redacted	Redacted

4. Operational Systems - Security Table:							
Name of System	Agency/ or Contractor Operated System?	NIST FIPS 199 Risk Impact level (High, Moderate, Low)	Has C&A been Completed, using NIST 800-37? (Y/N)	Date Completed: C&A	What standards were used for the Security Controls tests? (FIPS 200/NIST 800-53, Other, N/A)	Date Complete(d): Security Control Testing	Date the contingency plan tested
Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted	Redacted

5. Have any weaknesses, not yet remediated, related to any of the systems part of or supporting this investment been identified by the agency or IG? Yes

a. If "yes," have those weaknesses been incorporated into the agency's plan of action and milestone process? Yes

6. Indicate whether an increase in IT security funding is requested to remediate IT security weaknesses? Redacted

a. If "yes," specify the amount, provide a general description of the weakness, and explain how the funding request will remediate the weakness.

Amount: \$220,200

Weakness: This increased amount allocated from the straight-lined program budget is necessary to provide funding for the remediation of risks identified in a Plan of Action and Milestones (PO&AM) addressing implementation of e-authentication, IPv6, and HSPD-12 by FY09. This funding will be used to instantiate e-Authentication (an eGov initiative) in keeping with NIST 800-63 requirements that establish identity management capabilities for the investment's public facing web presence; implement IPv6 to achieve network-ready status for use across DOT network backbones, provide for new border perimeter security devices that are IPv6 compliant, and ensure that the investment's IP address space under IPv6 is sufficiently large to allow expansion of the user community and device count; and create a logical access capability for the investment that complies with NIST FIPS-201, 800-73r1 and 800-85A/B PIV standards required by HSPD-12.

Remediation: In FY 2008, NHTSA will complete an alternatives analysis for incorporating the requirements for HSPD-12, Infrastructure Optimization Initiative (IOI), IPv6, and e-Authentication initiatives (HOPE) into all of its IT investments. The analysis will evaluate the benefits, costs, and risks of accomplishing the HSPD-12, IPv6, and e-Authentication requirements separately or as an integral part of the Infrastructure Optimization and move to an authorized facility, as required by "DOT Information Technology Policy Number 0005-B: Authorized Hosting and Allocation of Relocation Resources and Infrastructure Support," dated May 11, 2007. As Artemis is already operating at an authorized facility, the first phase of the analysis will determine whether it should be included in the analysis, whether the single-site alternatives should focus on the site at which Artemis is hosted, or whether another alternative site should be considered and, if selected for other NHTSA investments currently at non-authorized sites, should also apply to Artemis.

7. How are contractor security procedures monitored, verified, and validated by the agency for the contractor systems above?

Redacted

8. Planning & Operational Systems - Privacy Table:					
(a) Name of System	(b) Is this a new system? (Y/N)	(c) Is there at least one Privacy Impact Assessment (PIA) which covers this system? (Y/N)	(d) Internet Link or Explanation	(e) Is a System of Records Notice (SORN) required for this system? (Y/N)	(f) Internet Link or Explanation
Artemis	No	Yes	http://www.dot.gov/pia/nhtsa_artemis.htm	No	No, because the system is not a Privacy Act system of records.

Details for Text Options:
 Column (d): If yes to (c), provide the link(s) to the publicly posted PIA(s) with which this system is associated. If no to (c), provide an explanation why the PIA has not been publicly posted or why the PIA has not been conducted.
 Column (f): If yes to (e), provide the link(s) to where the current and up to date SORN(s) is published in the federal register. If no to (e), provide an explanation why the SORN has not been published or why there isn't a current and up to date SORN.
 Note: Working links must be provided to specific documents not general privacy websites. Non-working links will be considered as a blank field.

Section F: Enterprise Architecture (EA) (IT Capital Assets only)

In order to successfully address this area of the capital asset plan and business case, the investment must be included in the agency's EA and Capital Planning and Investment Control (CPIC) process and mapped to and supporting the FEA. The business case must demonstrate the relationship between the investment and the business, performance, data, services, application, and technology layers of the agency's EA.

1. Is this investment included in your agency's target enterprise architecture? Yes

a. If "no," please explain why?

2. Is this investment included in the agency's EA Transition Strategy? Yes

a. If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment. Artemis

b. If "no," please explain why?

3. Is this investment identified in a completed (contains a No target architecture) and approved segment architecture?

a. If "yes," provide the name of the segment architecture as provided in the agency's most recent annual EA Assessment.

4. Service Component Reference Model (SRM) Table:								
Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov .								
Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
Data Cleansing	Support the maintenance and administration of data that describes data	Back Office Services	Data Management	Data Cleansing			No Reuse	2
Early Warning Reporting	Secure collection and processing of early warning reporting data submitted under 49 CFR Part 579.	Back Office Services	Data Management	Data Exchange			No Reuse	12
Back Up and Restore Services	Offsite tape storage of all Artemis databases and configuration files	Back Office Services	Data Management	Data Recovery			No Reuse	5
Data Warehouse	Defines the set of skills and capabilities that support the archiving and storage of large data volumes.	Back Office Services	Data Management	Data Warehouse			No Reuse	1
Optical Character Recognition	Process to extract machine editable text from scanned images.	Back Office Services	Data Management	Extraction and Transformation			No Reuse	2
Metis	To facilitate the collection, classification, visualization and maintenance of enterprise metadata.	Back Office Services	Data Management	Meta Data Management	Meta Data Management	021-18-03-00-02-3100-00	Internal	2
Rapid Application Development (RAD)	RAD will provide a component-based event-driven framework for developing web user interfaces.	Back Office Services	Development and Integration	Software Development	Software Development	021-18-03-00-02-3100-00	Internal	2
Discovery	Ad Hoc Reporting Tool	Business Analytical Services	Reporting	Ad Hoc			No Reuse	3
Standard Reports	Canned reports used to track status of investigations and recalls, investigator performance, EWR reporting, data quality, and industry.	Business Analytical Services	Reporting	Standardized / Canned			No Reuse	2
Appian	Manage the enterprise processes that support NHTSA and its policies; capture and execute business, manage process improvement, integrate existing systems and codify best practices.	Business Management Services	Management of Processes	Business Rule Management	Business Rule Management	021-18-03-00-02-3100-00	Internal	2
System Change	Module used by	Business	Management of	Change			No Reuse	2

4. Service Component Reference Model (SRM) Table:								
Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov .								
Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
Request Management	Configuration Control Board to manage and document system change requests for costing, approval, implementation, and acceptance testing.	Management Services	Processes	Management				
Source Safe Document/Configuration Management	Secure document management application to manage project design and requirements documents.	Business Management Services	Management of Processes	Configuration Management			No Reuse	2
Metis	Manage the enterprise processes, which support the organization and its policies.	Business Management Services	Management of Processes	Governance / Policy Management	Governance / Policy Management	021-18-03-00-02-3100-00	Internal	2
eRAMS	To assess risks for Artemis by identifying critical functions for project and security; assessing threats, vulnerabilities, consequences and mitigations; and assessing and prioritizing risks.	Business Management Services	Management of Processes	Risk Management	Risk Management	021-18-03-00-02-3100-00	Internal	2
Network Management	Support the detection of unauthorized access to information/data system.	Business Management Services	Organizational Management	Network Management	Network Management	021-18-02-00-02-4060-00	Internal	5
Help Desk Online	Online Help files integrated into each module to assist users in making the most use of the application.	Customer Services	Customer Initiated Assistance	Online Help			No Reuse	2
SFTP User Account Maintenance	Application to create and manage accounts for industry use of secure FTP server for EWR submissions.	Customer Services	Customer Relationship Management	Customer / Account Management			No Reuse	3
Content Publishing and Delivery	Allow for the propagation/transmission of interactive programs	Digital Asset Services	Content Management	Content Publishing and Delivery	Content Publishing and Delivery	021-18-03-00-02-3100-00	Internal	1
Repository	Storage Area Network for documents, images, video, and data files.	Digital Asset Services	Document Management	Library / Storage			No Reuse	5
Information Retrieval	Allow access to data and information for use by NHTSA and its stakeholders.	Digital Asset Services	Knowledge Management	Information Retrieval			No Reuse	0
Annotations	Integrated tool for capturing and sharing new information relevant to	Digital Asset Services	Knowledge Management	Information Sharing			No Reuse	5

4. Service Component Reference Model (SRM) Table:								
Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov .								
Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
	specific safety records such as complaints, recalls, investigations and EWR reports.							
Elements	Support the use of documents and data to be mined, abstracted and readily accessed among shareholders.	Digital Asset Services	Knowledge Management	Information Sharing	Information Sharing	021-18-03-00-02-3100-00	Internal	1
Knowledge Distribution and Delivery	Support the transfer of knowledge to DOT, Congress and the public.	Digital Asset Services	Knowledge Management	Knowledge Distribution and Delivery			No Reuse	1
Correspondence Management	Application for managing both incoming and outgoing correspondence.	Process Automation Services	Routing and Scheduling	Inbound Correspondence Management			No Reuse	5
Workflow	Integrated system to track, forward for approval, and edit case files for safety defect investigations.	Process Automation Services	Tracking and Workflow	Case Management			No Reuse	5
Oracle Portal and Forms	Custom Application to search and browse database for safety data including complaints, technical service bulletins, recalls, investigations, and EWR.	Support Services	Search	Query			No Reuse	6
Endeca	Support and leverage advance search capabilities; find information located in Artemis vast repository; search both unstructured and structured data; and identify connection and patterns within data.	Support Services	Search	Query	Information Retrieval	021-18-03-00-02-3100-00	Internal	1
Access Control	Support the management of permissions for login to Artemis applications, services, and network; includes user management and role/privilege management.	Support Services	Security Management	Access Control	Access Control	021-18-03-00-02-3100-00	Internal	2
Audit Trail	Integrated tool for tracking original field values and any changes made to include baseline values, changes, timestamp, and responsible user.	Support Services	Security Management	Audit Trail Capture and Analysis			No Reuse	2
Cyber Security Assessment and	CSAM will generate	Support Services	Security Management	FISMA Management	FISMA Management	021-18-02-00-02-4060-00	Internal	2

4. Service Component Reference Model (SRM) Table:								
Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov .								
Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
Management (CSAM)	management reports including enterprise, system, compliance and ad hoc reports; support all other security requirements			and Reporting	and Reporting			
Identification and Authentication	Support to acquire e-authentication login information about users attempting to log on to the ARTEMIS system for security purposes; and the validation of those users.	Support Services	Security Management	Identification and Authentication	Identification and Authentication		External	2
ISARM (Instrumented Situational Awareness Reporting Metric)	An intrusion detection method and technology designed to monitor service level security agreements for the purpose of validating contractor responsibilities to the government authorizing official (DAA) for the system they are managing.	Support Services	Security Management	Intrusion Detection	Risk Management	021-18-03-00-02-3100-00	Internal	2
IDS	Trainable intrusion detection system that monitors information requests and delivered packets searching for unusual transactions that may be the result of a hacker.	Support Services	Security Management	Intrusion Detection	Intrusion Detection	021-18-02-00-02-4060-00	Internal	2
Intrusion Detection	Support the detection of unauthorized access to ARTEMIS information/data system.	Support Services	Security Management	Intrusion Detection	Intrusion Detection	021-18-03-00-02-3100-00	Internal	2
Intrusion Prevention	Perform penetration testing and other measures to prevent unauthorized access to Artemis.	Support Services	Security Management	Intrusion Prevention	Intrusion Prevention	021-18-03-00-02-3100-00	Internal	2
Virus Protection	Provides anti-virus service to prevent, detect, and remediate infection of government computing assets.	Support Services	Security Management	Virus Protection	Virus Protection	021-18-02-00-02-4060-00	Internal	2
License Management	Defines the set of capabilities that support the purchase, refresh and tracking of legal	Support Services	Systems Management	License Management			No Reuse	1

4. Service Component Reference Model (SRM) Table:
 Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to <http://www.egov.gov>.

Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
	usage contracts for system software and applications.							

a. Use existing SRM Components or identify as "NEW". A "NEW" component is one not already identified as a service component in the FEA SRM.

b. A reused component is one being funded by another investment, but being used by this investment. Rather than answer yes or no, identify the reused service component funded by the other investment and identify the other investment using the Unique Project Identifier (UPI) code from the OMB Ex 300 or Ex 53 submission.

c. 'Internal' reuse is within an agency. For example, one agency within a department is reusing a service component provided by another agency within the same department. 'External' reuse is one agency within a department reusing a service component provided by another agency in another department. A good example of this is an E-Gov initiative service being reused by multiple organizations across the federal government.

d. Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the percentage of the BY requested funding amount transferred to another agency to pay for the service. The percentages in the column can, but are not required to, add up to 100%.

5. Technical Reference Model (TRM) Table:
 To demonstrate how this major IT investment aligns with the FEA Technical Reference Model (TRM), please list the Service Areas, Categories, Standards, and Service Specifications supporting this IT investment.

FEA SRM Component (a)	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (b) (i.e., vendor and product name)
Configuration Management	Component Framework	Business Logic	Platform Independent	Redacted
Information Sharing	Component Framework	Data Interchange	Data Exchange	Redacted
Query	Component Framework	Data Management	Reporting and Analysis	Redacted
Ad Hoc	Component Framework	Data Management	Reporting and Analysis	Redacted
Standardized / Canned	Component Framework	Data Management	Reporting and Analysis	Redacted
Information Sharing	Component Framework	Presentation / Interface	Content Rendering	Redacted
Software Development	Component Framework	Presentation / Interface	Dynamic Server-Side Display	Redacted
Network Management	Component Framework	Presentation / Interface	Static Display	Redacted
Access Control	Component Framework	Security	Certificates / Digital Signatures	Redacted
Access Control	Component Framework	Security	Certificates / Digital Signatures	Redacted
Intrusion Prevention	Component Framework	Security	Supporting Security Services	Redacted
FISMA Management and Reporting	Component Framework	Security	Supporting Security Services	Redacted
Risk Management	Component Framework	Security	Supporting Security Services	Redacted
Audit Trail Capture and Analysis	Component Framework	Security	Supporting Security Services	Redacted
Customer / Account Management	Component Framework	Security	Supporting Security Services	Redacted
Data Exchange	Component Framework	Security	Supporting Security Services	Redacted
Inbound Correspondence Management	Service Access and Delivery	Access Channels	Other Electronic Channels	Redacted
Information Retrieval	Service Access and Delivery	Access Channels	Web Browser	Redacted
Identification and Authentication	Service Access and Delivery	Service Requirements	Authentication / Single Sign-on	Redacted
Access Control	Service Access and Delivery	Service Requirements	Authentication / Single Sign-on	Redacted
Access Control	Service Access and Delivery	Service Requirements	Legislative / Compliance	Redacted
Content Publishing and Delivery	Service Access and Delivery	Service Transport	Service Transport	Redacted
Network Management	Service Access and Delivery	Service Transport	Service Transport	Redacted
Network Management	Service Access and Delivery	Service Transport	Service Transport	Redacted
Business Rule Management	Service Interface and Integration	Integration	Enterprise Application Integration	Redacted
Decision Support and Planning	Service Interface and Integration	Integration	Enterprise Application Integration	Redacted
Data Integration	Service Interface and Integration	Integration	Middleware	Redacted
Query	Service Interface and Integration	Interface	Service Description / Interface	Redacted
Extraction and Transformation	Service Interface and Integration	Interoperability	Data Transformation	Redacted
Data Warehouse	Service Platform and Infrastructure	Database / Storage	Database	Redacted
Library / Storage	Service Platform and	Database / Storage	Database	Redacted

5. Technical Reference Model (TRM) Table:				
To demonstrate how this major IT investment aligns with the FEA Technical Reference Model (TRM), please list the Service Areas, Categories, Standards, and Service Specifications supporting this IT investment.				
FEA SRM Component (a)	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (b) (i.e., vendor and product name)
	Infrastructure			
Meta Data Management	Service Platform and Infrastructure	Database / Storage	Storage	Redacted
Data Recovery	Service Platform and Infrastructure	Database / Storage	Storage	Redacted
Knowledge Distribution and Delivery	Service Platform and Infrastructure	Delivery Servers	Web Servers	Redacted
Intrusion Detection	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Redacted
Intrusion Detection	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Redacted
Access Control	Service Platform and Infrastructure	Hardware / Infrastructure	Local Area Network (LAN)	Redacted
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Redacted
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Redacted
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Redacted
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Redacted
Online Help	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Redacted
Change Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Redacted
License Management	Service Platform and Infrastructure	Support Platforms	Platform Dependent	Redacted
Case Management	Service Platform and Infrastructure	Support Platforms	Platform Independent	Redacted
Data Cleansing	Service Platform and Infrastructure	Support Platforms	Platform Independent	Redacted
Virus Protection	Service Platform and Infrastructure	Support Platforms	Platform Independent	Redacted
Intrusion Detection	Service Platform and Infrastructure	Support Platforms	Platform Independent	Redacted

a. Service Components identified in the previous question should be entered in this column. Please enter multiple rows for FEA SRM Components supported by multiple TRM Service Specifications

b. In the Service Specification field, agencies should provide information on the specified technical standard or vendor product mapped to the FEA TRM Service Standard, including model or version numbers, as appropriate.

6. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)? Yes

a. If "yes," please describe.

Artemis will leverage applications in the areas of risk management, PII protection, e-authentication, and HSPD-12 compliance. In addition, Artemis will also leverage the COE capabilities for antivirus, IDS, VPN and backup applications.

Exhibit 300: Part II: Planning, Acquisition and Performance Information

Section A: Alternatives Analysis (All Capital Assets)

Part II should be completed only for investments identified as "Planning" or "Full Acquisition," or "Mixed Life-Cycle" investments in response to Question 6 in Part I, Section A above.

In selecting the best capital asset, you should identify and consider at least three viable alternatives, in addition to the current baseline, i.e., the status quo. Use OMB Circular A-94 for all investments and the Clinger Cohen Act of 1996 for IT investments to determine the criteria you should use in your Benefit/Cost Analysis.

- 1. Did you conduct an alternatives analysis for this project? No
 - a. If "yes," provide the date the analysis was completed?
 - b. If "no," what is the anticipated date this analysis will be completed? 3/6/2006
 - c. If no analysis is planned, please briefly explain why:

2. Alternative Analysis Results:			* Costs in millions
Use the results of your alternatives analysis to complete the following table:			
Alternative Analyzed	Description of Alternative	Risk Adjusted Lifecycle Costs estimate	Risk Adjusted Lifecycle Benefits estimate
Redacted	Redacted	Redacted	Redacted
Redacted	Redacted	Redacted	Redacted
Redacted	Redacted	Redacted	Redacted
Redacted	Redacted	Redacted	Redacted

3. Which alternative was selected by the Agency's Executive/Investment Committee and why was it chosen?
Redacted

4. What specific qualitative benefits will be realized?
Redacted

- 5. Will the selected alternative replace a legacy system in-part or in-whole? No
 - a. If "yes," are the migration costs associated with the migration to the selected alternative included in this investment, the legacy investment, or in a separate migration investment.
 - b. If "yes," please provide the following information:

List of Legacy Investment or Systems		
Name of the Legacy Investment or Systems	UPI if available	Date of the System Retirement

Section B: Risk Management (All Capital Assets)

You should have performed a risk assessment during the early planning and initial concept phase of this investment's life-cycle, developed a risk-adjusted life-cycle cost estimate and a plan to eliminate, mitigate or manage risk, and be actively managing risk throughout the investment's life-cycle.

- 1. Does the investment have a Risk Management Plan? Yes
 - a. If "yes," what is the date of the plan? 7/10/2007
 - b. Has the Risk Management Plan been significantly changed since last year's submission to OMB? Yes
 - c. If "yes," describe any significant changes:

The new risk planning activities take into account the relocation of Artemis to the National Center for Critical Information Processing and Storage (NCCIPS) at the Stennis Space Center, Mississippi and the relocation of the majority of primary stakeholders to the new Southeast Federal Center in Washington DC. Both of these significant changes necessitate a complete review of risks in the areas of communication and security at a minimum.

- 2. If there currently is no plan, will a plan be developed?
 - a. If "yes," what is the planned completion date?

b. If "no," what is the strategy for managing the risks?

3. Briefly describe how investment risks are reflected in the life cycle cost estimate and investment schedule:

The life cycle cost estimate includes funds to mitigate risks associated with the agency's public website content management plans and style sheet standardization. The Artemis and SaferCar websites are being restyled to give the user a seamless experience when navigating the two sites. There are communication and scope creep risks associated with this plan and the lifecycle cost estimate includes funds to mitigate these risks to a degree if realized. Funds are also set aside to mitigate other risks such as applications changes necessitated by operating system or other critical security patches. Similarly, the investment schedule includes contingencies for unforeseen delays to absorb unforeseen delays.

Section C: Cost and Schedule Performance (All Capital Assets)

EVM is required only on DME portions of investments. For mixed lifecycle investments, O&M milestones should still be included in the table (Comparison of Initial Baseline and Current Approved Baseline). This table should accurately reflect the milestones in the initial baseline, as well as milestones in the current baseline.

1. Does the earned value management system meet the criteria in ANSI/EIA Standard-748? Yes

2. Is the CV% or SV% greater than +/- 10%? (CV%= CV/EV x 100; SV%= SV/PV x 100) No

a. If "yes," was it the CV or SV or both?

b. If "yes," explain the causes of the variance:

c. If "yes," describe the corrective actions:

3. Has the investment re-baselined during the past fiscal year? Yes

a. If "yes," when was it approved by the agency head? 8/13/2007

