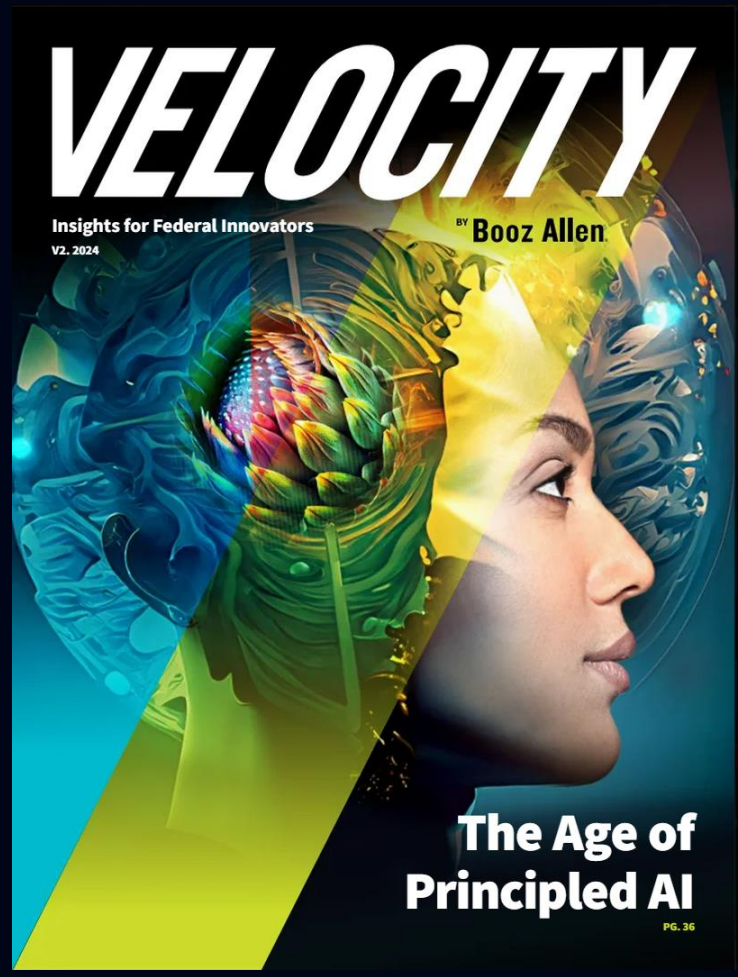
Booz Allen®

AI as a Service: Integration

28 AUG 24

OVERVIEW

- Primer – The Need for AI Integration
- AI Models Defined
- AI as a Service Use Case – IT Planning
- Additional Use Cases – Workflow, C2, ISR, Disconnected Operations
- A Closer Look
- Customize Your Experience / Needs
- Q&A



AI AS A "SERVICE INTEGRATOR"

BLUF: AI can't automate or solve everything. Rather, AI can automate pieces of most tasks, resulting in streamlined processes, increased throughput, and automation of repetitive, independent operations.

- Today, most systems, platforms, and AI-based services are constructed by OEMs/developers that provide various productivity workflow and analysis capabilities
- Each concentrates on their own specialized, contained, and controlled toolset, capability, or set of features with their own defined level of macro-enablement (or restricted versions) and interoperability
- These capabilities are then further siloed or compartmentalized into restricted, serial checkpoints, gateways, and access and traffic controls
- In many situations, however, users are required to use these capabilities to execute convoluted, process-driven tasks in support of productivity workflow and/or mission operations

Until now…

- Our AI as a Service model permits cross-talk over, and interoperability between, the separate realms
- Our synchronizing architecture relies on a bespoke planned and constructed Application Programming Interface (API) ecosystem that ties these disparate "realms" together to enable, traverse, and control/access to enable true, cross-environment interoperability

80% of the workforce could have at least **10%** of their work productivity affected by implementing AI models

20% of the workforce could see a positive impact to at least **50%** of their workload

15% of all work tasks in the U.S. could be completed significantly faster at the same level or result in higher quality and performance

UNDERSTANDING THE BASICS – AI/ML TERMINOLOGY

Algorithms

Recursive, Greedy, Backtracking, Sorting, Randomized

DEFINITION

A sequence of instructions that a computer must perform to solve a well-defined problem.

Recursive: Solves a particular problem by calling a copy of itself and solving smaller subproblems of the original problems

Greedy: Type of optimization algorithm that makes locally optimal choices at each step to find a globally optimal solution

Backtracking: Recursively explores all possible solutions to a problem

Sorting: Rearranges a given array or list of elements according to a comparison operator on the elements

Randomized: Uses randomness in computations to achieve a desired outcome

Auto Sum in Excel

AI Models

LLMs, LAMs, LMMs, LVMs

DEFINITION

Tools and algorithms used to train machines on datasets so that they may determine patterns, make conclusions, and help reach or execute decisions.

LLM: A form of artificial intelligence (AI) that can emulate human cognitive abilities by analyzing natural language patterns

LAM: Model that can understand and execute complex tasks by translating human intentions into action

LVM: AI model designed to analyze and comprehend visual information, primarily images or videos

LMM: to handle and generate content across multiple modalities, combining text with other forms of data such as images, audio, or video

ChatGPT, Google Lens, Rabbit AI

AI Frameworks

TensorFlow, PyTorch, Open AI

DEFINITION

A collection of pre-built tools and resources that simplify the process of building applications on the basis of artificial intelligence.

TensorFlow: Used to develop models for various tasks, including natural language processing, image recognition, handwriting recognition, and different computational-based simulations

PyTorch: Framework for building deep learning models, which is a type of machine learning that's commonly used in applications like image recognition and language processing

OpenAI: Range of tools for different AI tasks, including making images or converting text to speech; used for creating AI assistants or tools that interact with users in natural language

aiSSEMBLE, SW Development, Machine Learning

AI Agents

Simplex, Model-Based, Goal-Based, Utility, Learning

DEFINITION

Autonomous intelligent systems performing specific tasks without human intervention.

Simplex: Performs actions based on a current situation; scans knowledge base for how to respond to situations based on pre-determined rules

Model-Based: Uses condition-action rules to make decisions and act in real-time, based on their perception of the environment

Goal-Based: Goal-based agent attempts to choose the best strategy to achieve the objective based on the environment

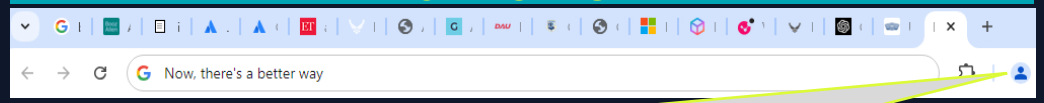
Utility: Agent that acts based not only on what the goal is but on the best way to reach that goal

Learning: Starts with basic knowledge and then acts and adapts autonomously, through learning, to improve its own performance

Virtual Assistants, Robotics, AI Applications

AI AS A SERVICE USE CASE

AI SERVICE MODEL



"I want to modernize my IT virtual/cloud infrastructure. I'll need to: Create a Digital Twin, assess changes to my system, and generate a BOM, cost estimate, and schedule; pre-populate, review, and stage both cyber and workflow documents for approval; perform capacity planning based on available work force, and assess supply availability."

- AI-enabled UI allows for change orchestration/automation
- Able to query and integrate data from multiple, AI-driven applications and models and COTS/GOTS-based services
- Absorbs, magnifies, returns, and applies data congruently

AGENT ADDAAM

- Autonomous, collaborative AI agents independently devise solutions to complex problems, working in tandem with users to achieve comprehensive and accurate results
- Domain expert; mimics user/executes queries (AI-enabled API)
- Inherits user permissions to access data (PKI authentication)
- Applies predictive analytics to optimize response time and accuracy
- Advanced Digital Decision Analysis and Actuation Model (ADDAAM)
- Analyzes RFI; applies appropriate AI model(s) to satisfy queries
- Enables Agent to traverse interconnective fabric, via an intuitive, pathfinding/navigating interfacial medium

Collaborative Efficiency. AI agents streamline task execution by managing multiple tasks simultaneously, fostering a collaborative environment where human intervention is minimized, and long-term efficiency gains are realized.

HOSTED ENVIRONMENT

- Cloud-hosted environment with proven tools, agile processes, workflows, cybersecurity, and full, multi-domain accreditation
- Pre-staged AI/ML algorithms and models (LMM, LAM, LVM)
- Secure, cross-ecosystem transit based upon destined routes (e.g., determined via Bayesian Occam's razor algorithm)

Adaptive Evolution. AI agents continuously evolve to solve increasingly complex tasks, enhancing their value and adaptability. They leverage advancements in AI models and tools, ensuring safety, security, and the generation data-driven insights.

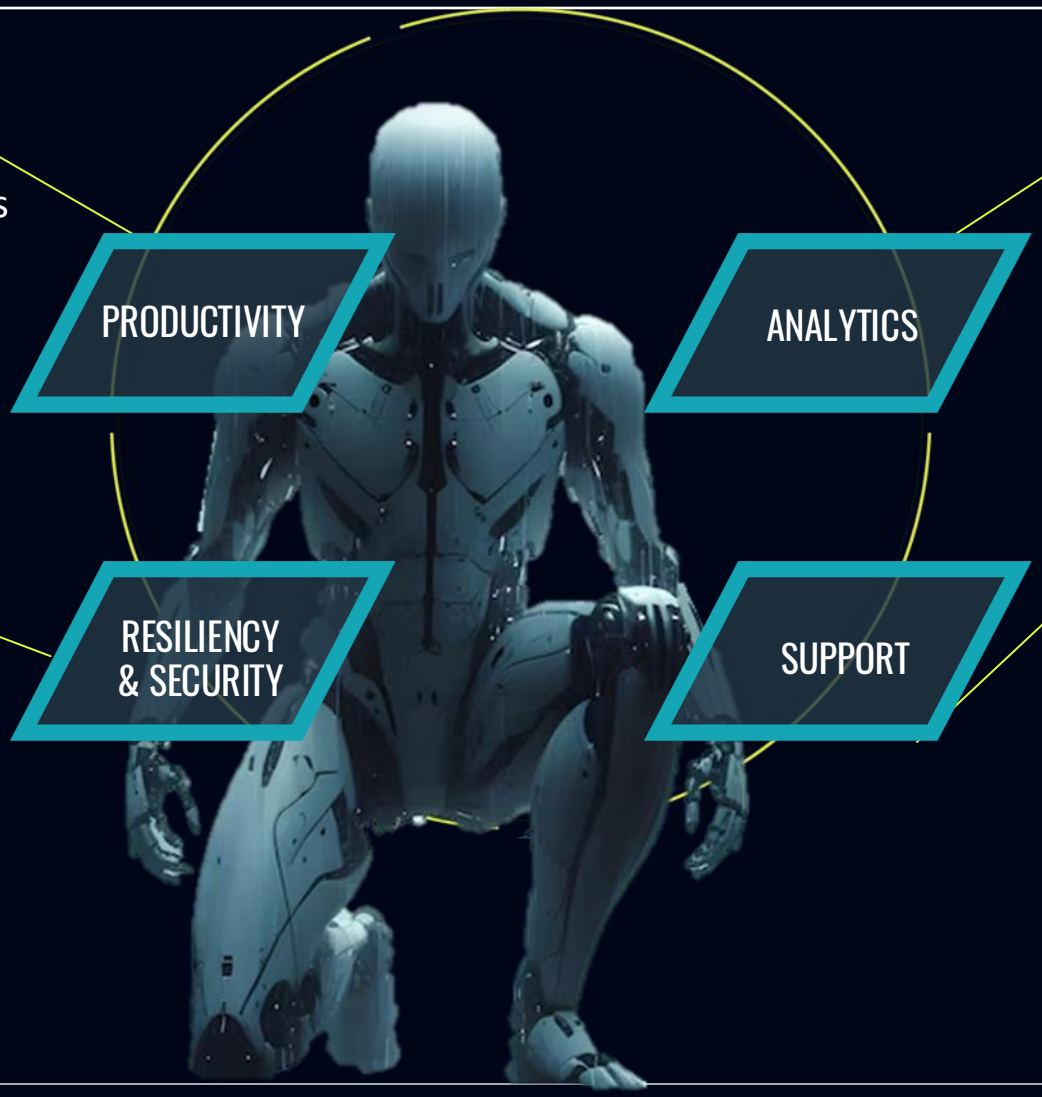
USE CASE APPLICABILITY

WORKFLOW

Automate independent queries via AI integration to fully connect, populate, and fuse data to enable enhanced interoperability.

CYBER

Multi-bot, comprehensive capability to aid practitioners in reducing time and errors while providing greater visibility in assessing overall security posture.



ISR

Utilizes ML and AI to deliver the right data in real-time to improve warfighter decision-making.

Service Desk

AI-powered chatbots and virtual assistants automate user support, leveraging NLP and ML to resolve queries swiftly and accurately.

OUR APPROACH TO AI INTEGRATION

1. User Input (Dev)

User makes a request through the AI agent application to generate an output (e.g., code). Through the management dashboard, the **business user** manages all agent functionality to control the permissions within the application, models being used, tools that are integrated, and data that can be accessed. A business leader's actions happen in parallel to the work being done by the AI agents.

2. Prompt Mgt

Improve contextual understanding by analyzing the conversation, a user's chat history, role, and stored data.

3. API Call to Model

Send user's input and contextual information to the model.

4. Model Orchestration

The agent communicates with itself, other agents, applications that it has access to, and long-term memory, which adds contextual information that the agent uses to plan and implement a solution.

5. Refinement

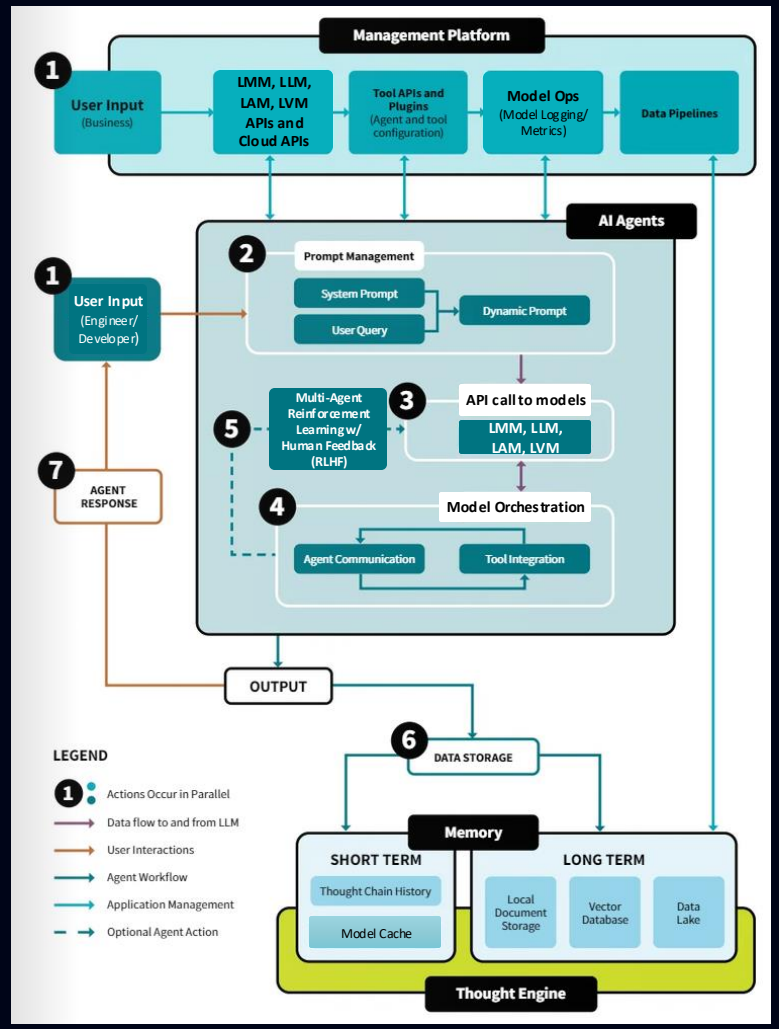
If needed, refine the response by sending it back to the model with specific instructions for solution improvement.

6. Data Storage

Save the final response and model output in the appropriate data resources.

7. Agent Response

The AI agent sends the output to the user, which can be in the form of text, code, or an action made within an integrated tool. The AI agent also outputs information to the management platform by logging relevant data and metrics.



Management Platform

At the core of AI agent operations lies the management layer, empowering both business and technical leaders with comprehensive control. This layer equips users with a robust set of tools to effectively oversee AI agent activities and user interactions. Key features encompass data management, integrations management, and model administration. In addition, it offers user permission controls, resource cost analysis, and API key management to ensure optimal utilization.

Memory

Enhancing the AI agents' proficiency is the memory layer, a repository of contextual information specific to tasks and enterprises. This layer grants AI agents access to an array of data stores ranging from structured to unstructured and vectorized formats. By augmenting the agents' knowledge with mission-critical insights, the memory layer significantly improves their overall performance. This contextual supplementation enables AI agents to deliver outputs that align precisely with the user's requirements.

AI Agents

The AI agents layer serves as the bridge between users' requests and meaningful outputs. Users input their requirements, such as tasks like developing Python scripts, resolving bugs, translating code, or submitting items like GitHub pull requests. These inputs are dynamically transformed into prompts that direct the AI agents' activities. The agents collaborate not only among themselves but also with integrated tools, generating valuable outputs for users. This layer also records comprehensive data, facilitating subsequent evaluation through the intuitive management dashboard.

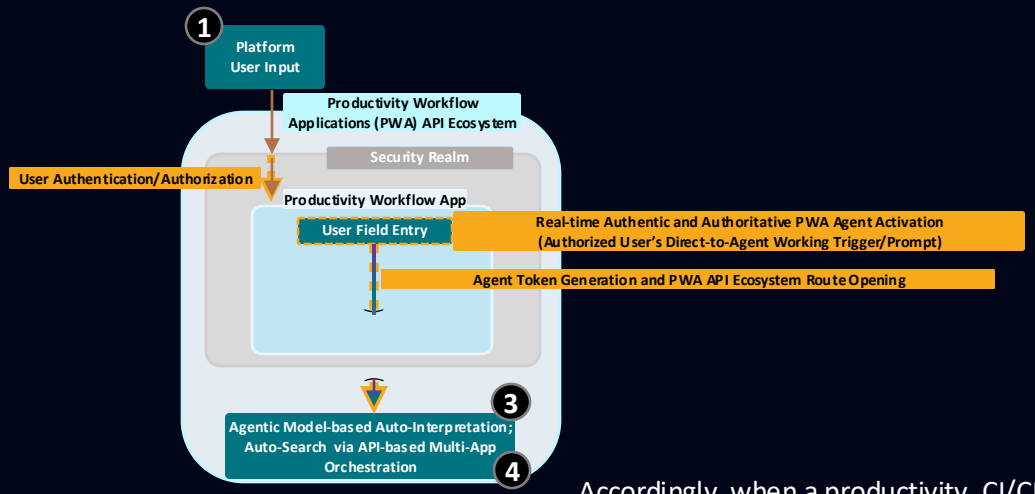
Thought Engine

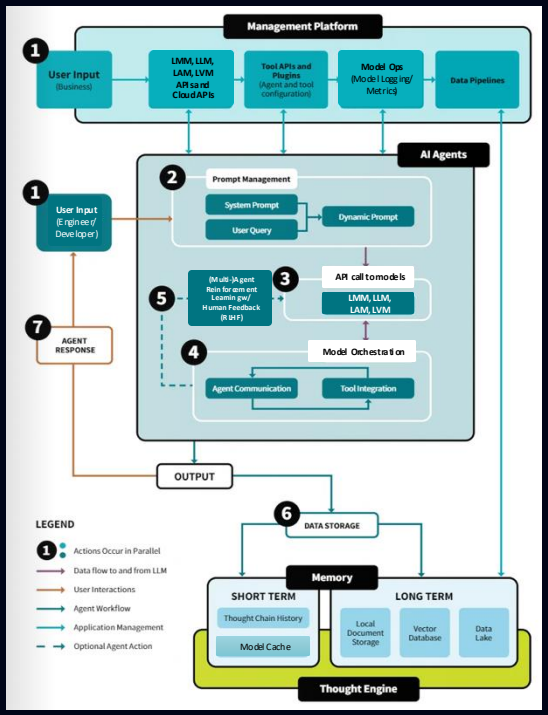
The hosting of the AI agent's application happens within the thought engine. This is a combination of cloud resources (which are multi-cloud compatible), local compute, and in-application processing.

OUR APPROACH TO AI INTEGRATION (CONT) – SECURITY AND ZERO TRUST

Securely tie segregated workflow applications/platforms while adhering to the zero-trust paradigm with automated agentic multi-platform access control. Across multiple applications/platforms (realms) that the user needs to pull data and artifacts from instantaneously, bypass the user's need to pull resources on a realm-by-realm basis. The agent will reduce compute overhead in the number of windows or tabbed instances of a browser maintained (in machine memory) and tracked (via human memory) during normal workflow processes via an API-based chain of multi-platform access.

SECURITY CONSIDERATION





Accordingly, when a productivity, CI/CD app user begins drafting a ticket in a change processing app (consistent with step 1 above), the AI agent receives requisite token(s), establishes token-enabled routing, begins interpreting (à la step 3) the field entry(ies), and explores the API ecosystem *while authentic authority is activated* to orchestrate productivity workflow activities based upon interpretation(s) (moving straight into model orchestration, which is step 4) by accessing and searching other apps/tools sequentially for helpful artifacts or jumpstarting parallel product change-related acts, reducing human context switching and client machine processing load. Post-orchestration, the agent enters RHFL refinement (i.e., step 5 on the previous slide).

CUSTOMIZE TO YOUR NEEDS

PREPARE

- Conduct strategic evaluation that gauges current Intelligent Automation (IA) capabilities
- Provide a roadmap for development
- Assess readiness for adopting or expanding IA technologies
- Allow for strategies to overcome potential barriers
- Collect data through multiple mediums before analyzing and sharing across the organization
- Research for insight into the customer, their values, and their interactions within the organization

DESIGN

- Analyze your organization's processes and pinpoint areas for maximum IA impact
- Design blueprints for successful IA system integration into existing IT infrastructure
- Ensure seamless interoperability with minimized disruption, which equals maximized utility
- Improve interactions with customers and the underlying operations which shape service delivery

DEVELOP

- Provide specialized, tailored (artificial intelligence) AI solutions for your unique needs
- Design and train AI models that efficiently automate complex tasks, enhance decision making, and drive operational improvements
- Utilize advanced analytics to help the process, identify inefficiencies, and improve overall productivity and speed
- Develop, deploy, and seamlessly integrate systems to create unified experiences

OPTIMIZE

- Keep detailed monitoring of performance and accuracy
- Help scale AI models, retrain with relevant data, and enable models to adapt to an evolving landscape
- Maintain the integrity of the data used in training/testing AI models
- Clarify decision-making process of complex AI models by developing interpretation methods while incorporating explainability
- Introduce new solutions to customers, employees, and stakeholders
- Customer feedback is received, and issues are identified and resolved to maintain long-term positive relationships

AI ENHANCEMENTS

- Use natural language processing techniques and AI models to resolve large amounts of data
- Use AI to create personas to interact with customers

AI PRODUCTS

- Design AI agents that seamlessly integrate to aid humans in end-to-end service deliveries
- Address key points and enhance customer experience

IMPLEMENTATION

- Integrate AI tools across software development lifecycles to increase productivity of agile development teams
- Use LLMs to integrate advanced self-service and on-demand resources to assist users in navigating change

ENGAGEMENT

- Use AI agents to route and prioritize customer requests and use natural language processing for analysis

- **Proven strategy:** We assess each user's needs, goals, and unique situation to ensure the fastest results with the highest value, efficiency, and cost-effectiveness.

- **Holistic perspective:** Whether the goal is to accelerate software production, ensure compliance with new digital policies, transition securely to the cloud, or another mission, we look at the whole problem to ensure the technology aligns with people, processes, and policies.

- **Innovative tech stack:** Our base digital engineering tech stack jump-starts client projects with proven tools, agile processes, workflows, embedded cybersecurity, and full accreditation.

- **Agile ecosystem:** We use a modular open systems architecture (MOSA) to ensure flexibility, adaptability, and client ownership—while driving digital integration.

Booz Allen AI Innovation

- Booz Allen Deploys the Power of Generative AI in Space
- Booz Allen Leads AI Deployment for U.S. Government
- Booz Allen Helps U.S. Air Force Give Flight to AI Copilot
- Velocity by Booz Allen

DISCUSSION

Q&A

LIZZ SAID
Principal/Director
Digital Battlespace
said_lizz@bah.com

JONATHAN WASILEWSKI
Chief Technologist
Digital Battlespace
wasilewski_jonathan@bah.com

ALAN HEYWARD
Sr Lead Technologist
Digital Battlespace
heyward_alan@bah.com

DAVID "REED" CRUMLEY
Sr Lead Technologist
Digital Battlespace
crumley_david@bah.com

Booz Allen